



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.5.1

MAY 8, 2025

EFFECTIVE DATE

(05-08-2025)

PURPOSE

- (1) This transmits revised IRM 10.5.1, Privacy and Information Protection, Privacy Policy.

BACKGROUND

- (1) IRM 10.5.1, Privacy Policy, is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Privacy and Information Protection.

MATERIAL CHANGES

- (1) IRM 10.5.1.1.1, Purpose of the Program, updated the Privacy, Governmental Liaison and Disclosure (PGLD) vision and mission statements. Referenced Treasury Senior Agency Official for Privacy.
- (2) IRM 10.5.1.1.5, Background, clarified existing subsection references and the term “includes.”
- (3) IRM 10.5.1.2.2.1, Examples and Categories of SBU Data, added clarity on existing sensitivity marking options.
- (4) IRM 10.5.1.2.2.2, Official Use Only (OUO) and Limited Official Use, added exception to cross-reference publishing use of OUO for clarity.
- (5) IRM 10.5.1.2.3, Personally Identifiable Information (PII), added clarity on existing sensitivity marking options.
- (6) IRM 10.5.1.2.4, Federal Tax Information (FTI), added clarity on existing sensitivity marking options.
- (7) IRM 10.5.1.3.2, IRS Privacy Principles, added reference to existing Privacy Act requirement.
- (8) IRM 10.5.1.4.7, Personnel in Contract Activities, renamed and incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (9) IRM 10.5.1.6.1.4, Synthetic or Fictitious Data, added new subsection to clarify and reference existing requirements.
- (10) IRM 10.5.1.6.2, Encryption, incorporated PGLD-10-0724-0016, Privacy Policy Encryption Updates.
- (11) IRM 10.5.1.6.5, Marking, added clarity on existing sensitivity marking options.
- (12) IRM 10.5.1.6.7, Phone, incorporated PGLD-10-0424-0011, Text Messaging Privacy.
- (13) IRM 10.5.1.6.8, Email and Other Electronic Communications, incorporated PGLD-10-0724-0016, Privacy Policy Encryption Updates.
- (14) IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives, incorporated PGLD-10-0724-0016, Privacy Policy Encryption Updates.
- (15) IRM 10.5.1.6.8.2, Emails to Other External Stakeholders, incorporated PGLD-10-0724-0016, Privacy Policy Encryption Updates.
- (16) IRM 10.5.1.6.8.3, Emails to IRS Accounts, incorporated PGLD-10-0724-0016, Privacy Policy Encryption Updates.

- (17) IRM 10.5.1.6.8.4, Emails with Personal Accounts, incorporated PGLD-10-0724-0016, Privacy Policy Encryption Updates.
- (18) IRM 10.5.1.6.8.5, Limited Exceptions to Email SBU Data Encryption, incorporated PGLD-10-0724-0016, Privacy Policy Encryption Updates.
- (19) IRM 10.5.1.6.9.2, Mail through United States Postal Service (USPS), renamed and clarified existing policy to use USPS for all mail sent to taxpayers and their representatives.
- (20) IRM 10.5.1.6.9.3, Shipping through Private Delivery Carrier, clarified existing Form 3210 requirements.
- (21) IRM 10.5.1.6.9.6, Text Messaging (Texting), incorporated PGLD-10-0424-0011, Text Messaging Privacy.
- (22) IRM 10.5.1.6.14.2, Recordings in the Workplace, clarified existing requirements for recording around business need, approval, consent, precautions, and government equipment. Added exception to reflect existing policy for emergency recording of threats.
- (23) IRM 10.5.1.6.15, Contracts, renamed and incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (24) IRM 10.5.1.6.15.1, Contract Privacy Requirements Language, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (25) IRM 10.5.1.6.15.2, Contracting Officer's Representative (COR) Training, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (26) IRM 10.5.1.6.15.3, OneSDLC in Contracts, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (27) IRM 10.5.1.6.15.4, Privacy Act in Contracts, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (28) IRM 10.5.1.6.15.5, IRC 6103 (Tax Information) in Contracts, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (29) IRM 10.5.1.6.15.6, Background Investigation, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (30) IRM 10.5.1.6.15.7, Mandatory Training for Contractors, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (31) IRM 10.5.1.6.15.8, Non-Disclosure Agreements, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (32) IRM 10.5.1.6.15.9, Privacy and Security Controls in Contracts, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (33) IRM 10.5.1.6.15.10, Privacy and Civil Liberties Impact Assessments (PCLIAAs) in Contracts, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (34) IRM 10.5.1.6.15.11, Testing and Development Environments in Contracts, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (35) IRM 10.5.1.6.15.12, Incident Response in Contracts, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.

- (36) IRM 10.5.1.6.15.13, Unauthorized Access (UNAX) in Contracts, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (37) IRM 10.5.1.6.15.14, Contract Closeout, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (38) IRM 10.5.1.6.15.15, Federal Acquisition Regulation (FAR) Compliance, new subsection from incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (39) IRM 10.5.1.6.16, Online Data Collection and Privacy Notices, incorporated PGLD-10-0224-0004, Online Privacy Notices.
- (40) IRM 10.5.1.6.16.1, IRS.gov Privacy Policy Notice, incorporated PGLD-10-0224-0004, Online Privacy Notices.
- (41) IRM 10.5.1.6.16.2, Online Data Collection Privacy Act Statement, renamed and incorporated PGLD-10-0224-0004, Online Privacy Notices.
- (42) IRM 10.5.1.6.16.3, Privacy Departure Notice, incorporated PGLD-10-0224-0004, Online Privacy Notices.
- (43) IRM 10.5.1.6.16.4, Internal Websites and Digital Services Privacy Policy and Privacy Act Statement, renamed and incorporated PGLD-10-0224-0004, Online Privacy Notices.
- (44) IRM 10.5.1.6.18.4, Cloud Computing, added clarification from existing policy and new OMB memo.
- (45) IRM 10.5.1.6.22, Artificial Intelligence (AI), new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (46) IRM 10.5.1.6.22.1, Accountability for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (47) IRM 10.5.1.6.22.2, Purpose Limitation for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (48) IRM 10.5.1.6.22.3, Minimizing Collection, Use, Retention, and Disclosure for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (49) IRM 10.5.1.6.22.4, Openness and Consent for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (50) IRM 10.5.1.6.22.5, Strict Confidentiality for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (51) IRM 10.5.1.6.22.6, Security for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (52) IRM 10.5.1.6.22.7, Data Quality for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (53) IRM 10.5.1.6.22.8, Verification and Notification for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (54) IRM 10.5.1.6.22.9, Access, Correction, and Redress for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.
- (55) IRM 10.5.1.6.22.10, Privacy Awareness and Training for AI, new subsection from incorporated PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence.

- (56) IRM 10.5.1.7.4, Privacy Control Assessment Teams (PCAT), new subsection to reference existing program.
- (57) IRM 10.5.1.7.19.2, Creating and Revising IRS Products, new subsection from incorporated PGLD-10-1123-0006, Interim Guidance: New Procedures for Creating and Revising IRS Products that Contain Social Security Numbers (SSNs) and/or Tax Identification Numbers (TINs).
- (58) IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls, and all of its subsections: Updated single-digit control numbers to include leading 0 to match NIST convention. Changed privacy concerns language to IRS requirements language. Improved formatting of implementation guidance and IRM references.
- (59) IRM 10.5.1.8.10.13, PM-17 Program Management -- Protecting Controlled Unclassified Information on External Systems [J] {Org}, incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (60) IRM 10.5.1.8.10.14, PM-18 Program Management — Privacy Program Plan [P] {Org}, updated existing control language for clarity.
- (61) IRM 10.5.1.8.10.22, PM-25 Program Management — Minimization of Personally Identifiable Information Used for Testing, Training, and Research [P] {Org}, updated existing control language for clarity.
- (62) IRM 10.5.1.8.10.23, PM-26 Program Management — Complaint Management [P] {Org}, updated existing control language for clarity.
- (63) IRM 10.5.1.8.12, PT-01 Personally Identifiable Information Processing and Transparency — Policy and Procedures [P] {Org}, updated existing control language for clarity.
- (64) IRM 10.5.1.8.12.1, PT-02 Personally Identifiable Information Processing and Transparency — Authority to Process Personally Identifiable Information [P] {Org}, updated existing control language for clarity.
- (65) IRM 10.5.1.8.12.4, PT-05 Personally Identifiable Information Processing and Transparency — Privacy Notice [P] {Hybrid}, updated existing control language for clarity.
- (66) IRM 10.5.1.8.14.3, SA-04 System and Services Acquisition – Acquisition Process [J] {Sys}, incorporated PGLD-10-1024-0021, Contract Privacy Requirements.
- (67) IRM 10.5.1.8.16.3, SI-12(2) System and Information Integrity — Information Management and Retention - Minimize Personally Identifiable Information in Testing, Training, and Research [P] {Sys}, updated existing control language for clarity.
- (68) Throughout the IRM, made editorial changes to existing policy for clarification, updated or added links, references, citations, and organization names, corrected content for style, grammar, and plain language, moved some existing note content to paragraphs, and converted existing long or complicated lists to paragraphs or tables for clarity.
- (69) IRM 10.5.1 has been updated to comply with January 2025 Executive Orders and OPM guidance.

EFFECT ON OTHER DOCUMENTS

This version supersedes IRM 10.5.1, Privacy Policy, dated September 15, 2023. Also, this IRM supports other IRMs in the IRM 10.5 series. This IRM incorporates Interim Guidance Memoranda:

- PGLD-10-1123-0006, Interim Guidance: New Procedures for Creating and Revising IRS Products that Contain Social Security Numbers (SSNs) and/or Tax Identification Numbers (TINs), dated 11/15/2023
- PGLD-10-0224-0004, Online Privacy Notices, dated 02/26/2024
- PGLD-10-0424-0011, Text Messaging Privacy, dated 04/26/2024

- PGLD-10-0724-0016, Privacy Policy Encryption Updates, dated 07/08/2024
- PGLD-10-0924-0020, Privacy Policy for Artificial Intelligence, dated 09/30/2024
- PGLD-10-1024-0021, Contract Privacy Requirements, dated 10/23/2024

AUDIENCE

IRM 10.5.1 addresses IRS personnel responsible for ensuring adequate privacy and information protection for all sensitive but unclassified (SBU) data, including tax information and personally identifiable information (PII). This policy applies to all IRS personnel, as defined in this IRM.

John E. Lyons
Director, Privacy Policy and Compliance (PPC)

10.5.1
Privacy Policy

Table of Contents

- 10.5.1.1 Program Scope and Objectives
 - 10.5.1.1.1 Purpose of the Program
 - 10.5.1.1.2 Audience
 - 10.5.1.1.3 Policy and Program Owners
 - 10.5.1.1.4 Primary Stakeholders
 - 10.5.1.1.5 Background
 - 10.5.1.1.6 Authority
 - 10.5.1.1.7 Roles and Responsibilities
 - 10.5.1.1.8 Program Management and Review
 - 10.5.1.1.9 Program Controls
 - 10.5.1.1.10 Terms and Acronyms
 - 10.5.1.1.11 Related Resources
- 10.5.1.2 Key Privacy Definitions
 - 10.5.1.2.1 Privacy Lifecycle
 - 10.5.1.2.2 Sensitive But Unclassified (SBU) Data
 - 10.5.1.2.2.1 Examples and Categories of SBU Data
 - 10.5.1.2.2.2 Official Use Only and Limited Official Use
 - 10.5.1.2.2.3 Freedom of Information Act (FOIA) and SBU Data
 - 10.5.1.2.3 Personally Identifiable Information (PII)
 - 10.5.1.2.3.1 Examples and Categories of PII
 - 10.5.1.2.3.2 Public Record
 - 10.5.1.2.3.3 Defining PII versus Sensitive PII
 - 10.5.1.2.4 Federal Tax Information (FTI)
 - 10.5.1.2.5 UNAX
 - 10.5.1.2.6 Unauthorized Access of SBU Data
 - 10.5.1.2.7 Privacy Act Information
 - 10.5.1.2.8 Need To Know
 - 10.5.1.2.9 Authentication
 - 10.5.1.2.10 Authorization
 - 10.5.1.2.11 High Security Items
- 10.5.1.3 Key Privacy Concepts
 - 10.5.1.3.1 Privacy Controls
 - 10.5.1.3.2 IRS Privacy Principles
 - 10.5.1.3.2.1 Accountability
 - 10.5.1.3.2.2 Purpose Limitation

-
- 10.5.1.3.2.3 Minimizing Collection, Use, Retention, and Disclosure
 - 10.5.1.3.2.4 Openness and Consent
 - 10.5.1.3.2.5 Strict Confidentiality
 - 10.5.1.3.2.6 Security
 - 10.5.1.3.2.7 Data Quality
 - 10.5.1.3.2.8 Verification and Notification
 - 10.5.1.3.2.9 Access, Correction, and Redress
 - 10.5.1.3.2.10 Privacy Awareness and Training
 - 10.5.1.4 IRS-Wide Privacy Roles and Responsibilities
 - 10.5.1.4.1 Employees and Personnel
 - 10.5.1.4.2 Management
 - 10.5.1.4.3 Senior Management and Executives
 - 10.5.1.4.4 System Owners
 - 10.5.1.4.5 System Developers
 - 10.5.1.4.6 Authorizing Officials
 - 10.5.1.4.7 Personnel in Contract Activities
 - 10.5.1.5 Privacy Culture
 - 10.5.1.5.1 Clean Desk Policy
 - 10.5.1.5.2 Privacy in Practice (PiP)
 - 10.5.1.6 Practical Privacy Policy
 - 10.5.1.6.1 Protecting and Safeguarding SBU Data
 - 10.5.1.6.1.1 Deciding Risk Levels for SBU Data
 - 10.5.1.6.1.2 Limiting Sharing of SBU Data
 - 10.5.1.6.1.3 Extracting SBU Data
 - 10.5.1.6.1.4 Synthetic or Fictitious Data
 - 10.5.1.6.2 Encryption
 - 10.5.1.6.3 Computers and Mobile Computing Devices
 - 10.5.1.6.4 Data Loss
 - 10.5.1.6.5 Marking
 - 10.5.1.6.6 Storage
 - 10.5.1.6.7 Phone
 - 10.5.1.6.7.1 Cell Phone or Cordless Device
 - 10.5.1.6.7.2 Answering Machine or Voicemail
 - 10.5.1.6.8 Email and Other Electronic Communications
 - 10.5.1.6.8.1 Emails to Taxpayers and Representatives
 - 10.5.1.6.8.2 Emails to Other External Stakeholders
 - 10.5.1.6.8.3 Emails to IRS Accounts
 - 10.5.1.6.8.4 Emails with Personal Accounts
 - 10.5.1.6.8.5 Limited Exceptions to Email SBU Data Encryption

-
- 10.5.1.6.8.6 Other Secure Electronic Communication Methods
 - 10.5.1.6.9 Other Forms of Transmission
 - 10.5.1.6.9.1 Field and Travel
 - 10.5.1.6.9.2 Mail through United States Postal Service (USPS)
 - 10.5.1.6.9.3 Shipping through Private Delivery Carrier
 - 10.5.1.6.9.4 Faxing
 - 10.5.1.6.9.5 Printing
 - 10.5.1.6.9.6 Text Messaging (Texting)
 - 10.5.1.6.9.7 Electronic and Online
 - 10.5.1.6.9.8 Information Privacy During Office Moves
 - 10.5.1.6.10 Disposition and Destruction
 - 10.5.1.6.10.1 Hardcopy Paper Disposition and Destruction
 - 10.5.1.6.10.2 Electronic Disposition and Destruction
 - 10.5.1.6.10.3 Microforms Disposition and Destruction
 - 10.5.1.6.10.4 Temporary Storage Disposition and Destruction
 - 10.5.1.6.10.5 Records Management Disposition and Destruction
 - 10.5.1.6.10.6 Contractors Disposition and Destruction
 - 10.5.1.6.10.7 Recycling Disposition and Destruction
 - 10.5.1.6.11 Global Positioning Systems (GPS) and Location Services
 - 10.5.1.6.11.1 Global Positioning Systems (GPS)
 - 10.5.1.6.11.2 Location Services
 - 10.5.1.6.12 Telework
 - 10.5.1.6.13 Bring Your Own Device (BYOD)
 - 10.5.1.6.14 Civil Liberties
 - 10.5.1.6.14.1 First Amendment
 - 10.5.1.6.14.2 Recordings in the Workplace
 - 10.5.1.6.14.3 Monitoring Individuals
 - 10.5.1.6.15 Contracts
 - 10.5.1.6.15.1 Contract Privacy Requirements Language
 - 10.5.1.6.15.2 Contracting Officer's Representative (COR) Training
 - 10.5.1.6.15.3 OneSDLC in Contracts
 - 10.5.1.6.15.4 Privacy Act in Contracts
 - 10.5.1.6.15.5 IRC 6103 (Tax Information) in Contracts
 - 10.5.1.6.15.6 Background Investigation
 - 10.5.1.6.15.7 Mandatory Training for Contractors
 - 10.5.1.6.15.8 Non-Disclosure Agreements
 - 10.5.1.6.15.9 Privacy and Security Controls in Contracts
 - 10.5.1.6.15.10 Privacy and Civil Liberties Impact Assessment (PCLIA) in Contracts
 - 10.5.1.6.15.11 Testing and Development Environments in Contracts

-
- 10.5.1.6.15.12 Incident Response in Contracts
 - 10.5.1.6.15.13 Unauthorized Access (UNAX) in Contracts
 - 10.5.1.6.15.14 Contract Closeout
 - 10.5.1.6.15.15 Federal Acquisition Regulation (FAR) Compliance
 - 10.5.1.6.16 Online Data Collection and Privacy Notices
 - 10.5.1.6.16.1 IRS.gov Privacy Policy Notice
 - 10.5.1.6.16.2 Online Data Collection Privacy Act Statement
 - 10.5.1.6.16.3 Privacy Departure Notice
 - 10.5.1.6.16.4 Internal Websites and Digital Services Privacy Policy and Privacy Act Statement
 - 10.5.1.6.17 Social Media
 - 10.5.1.6.18 Data on Collaborative Technology and Systems
 - 10.5.1.6.18.1 Shared Calendar
 - 10.5.1.6.18.2 Online Meetings
 - 10.5.1.6.18.3 Shared IRS Storage (OneDrive, SharePoint, Teams, and Other IRS Collaborative Sites)
 - 10.5.1.6.18.4 Cloud Computing
 - 10.5.1.6.19 Training
 - 10.5.1.6.20 Smart Devices
 - 10.5.1.6.21 Biometric Technology
 - 10.5.1.6.22 Artificial Intelligence (AI)
 - 10.5.1.6.22.1 Accountability for AI
 - 10.5.1.6.22.2 Purpose Limitation for AI
 - 10.5.1.6.22.3 Minimizing Collection, Use, Retention, and Disclosure for AI
 - 10.5.1.6.22.4 Openness and Consent for AI
 - 10.5.1.6.22.5 Strict Confidentiality for AI
 - 10.5.1.6.22.6 Security for AI
 - 10.5.1.6.22.7 Data Quality for AI
 - 10.5.1.6.22.8 Verification and Notification for AI
 - 10.5.1.6.22.9 Access, Correction, and Redress for AI
 - 10.5.1.6.22.10 Privacy Awareness and Training for AI
 - 10.5.1.7 Privacy-Related Programs
 - 10.5.1.7.1 IRS Privacy Council
 - 10.5.1.7.2 Privacy and Civil Liberties Impact Assessment (PCLIA)
 - 10.5.1.7.3 Business PII Risk Assessment (BPRA)
 - 10.5.1.7.4 Privacy Control Assessment Teams (PCAT)
 - 10.5.1.7.5 Privacy Reporting
 - 10.5.1.7.6 UNAX Program
 - 10.5.1.7.7 Mandatory Briefings
 - 10.5.1.7.8 Records and Information Management (RIM)
 - 10.5.1.7.9 Disclosure

- 10.5.1.7.10 Digital Identity Risk Assessment (DIRA)
- 10.5.1.7.11 One Solution Delivery Life Cycle (OneSDLC)
- 10.5.1.7.12 Governmental Liaison (GL)
- 10.5.1.7.13 Data Services
- 10.5.1.7.14 Identity Assurance (IA)
 - 10.5.1.7.14.1 Electronic Signature (e-Signature) Program
 - 10.5.1.7.14.2 Non-Digital Authentication Risk Assessment (NDARA)
- 10.5.1.7.15 IT Security
- 10.5.1.7.16 Incident Management (IM)
- 10.5.1.7.17 Pseudonym
- 10.5.1.7.18 Safeguards
- 10.5.1.7.19 Social Security Number Elimination and Reduction (SSN ER)
 - 10.5.1.7.19.1 Acceptable Use of SSNs
 - 10.5.1.7.19.2 Creating and Revising IRS Products
 - 10.5.1.7.19.3 SSN Necessary-Use Criteria
- 10.5.1.7.20 SBU Data Use for Non-Production Environments
- 10.5.1.7.21 Quick Response (QR) Codes
- 10.5.1.8 NIST SP 800-53 Security and Privacy Controls
 - 10.5.1.8.1 AC-01 Access Control — Policy and Procedures [J] {Org}
 - 10.5.1.8.1.1 AC-03(14) Access Control — Access Enforcement - Individual Access [P] {Org}
 - 10.5.1.8.2 AT-01 Awareness and Training — Policy and Procedures [J] {Org}
 - 10.5.1.8.2.1 AT-02 Awareness and Training — Literacy Training and Awareness [J] {Org}
 - 10.5.1.8.2.2 AT-03 Awareness and Training — Role-Based Training [J] {Org}
 - 10.5.1.8.2.3 AT-03(5) Awareness and Training — Role-Based Training - Processing Personally Identifiable Information [P] {Org}
 - 10.5.1.8.2.4 AT-04 Awareness and Training — Training Records [J] {Org}
 - 10.5.1.8.3 AU-01 Audit and Accountability — Policy and Procedures [J] {Org}
 - 10.5.1.8.3.1 AU-02 Audit and Accountability — Event Logging [J] {Org}
 - 10.5.1.8.3.2 AU-03(3) Audit and Accountability — Content of Audit Records - Limit Personally Identifiable Information Elements [P] {Sys}
 - 10.5.1.8.3.3 AU-11 Audit and Accountability — Audit Record Retention [J] {Org}
 - 10.5.1.8.4 CA-01 Assessment Authorization and Monitoring — Policy and Procedures [J] {Org}
 - 10.5.1.8.4.1 CA-02 Assessment Authorization and Monitoring — Control Assessments [J] {Sys}
 - 10.5.1.8.4.2 CA-05 Assessment Authorization and Monitoring — Plan of Action and Milestones [J] {Sys}
 - 10.5.1.8.4.3 CA-06 Assessment Authorization and Monitoring — Authorization [J] {Sys}
 - 10.5.1.8.4.4 CA-07 Assessment Authorization and Monitoring — Continuous Monitoring [J] {Org}
 - 10.5.1.8.4.5 CA-07(4) Assessment Authorization and Monitoring — Continuous Monitoring - Risk Monitoring [J] {Org}
 - 10.5.1.8.5 CM-01 Configuration Management — Policy and Procedures [J] {Org}

- 10.5.1.8.5.1 CM-04 Configuration Management — Impact Analysis [J] {Sys}
- 10.5.1.8.6 IR-01 Incident Response — Policy and Procedures [J] {Org}
 - 10.5.1.8.6.1 IR-02 Incident Response — Incident Response Training [J] {Org}
 - 10.5.1.8.6.2 IR-02(3) Incident Response — Incident Response Training - Breach [P] {Org}
 - 10.5.1.8.6.3 IR-03 Incident Response — Incident Response Testing [J] {Org}
 - 10.5.1.8.6.4 IR-04 Incident Response — Incident Handling [J] {Org}
 - 10.5.1.8.6.5 IR-05 Incident Response — Incident Monitoring [J] {Org}
 - 10.5.1.8.6.6 IR-06 Incident Response — Incident Reporting [J] {Org}
 - 10.5.1.8.6.7 IR-07 Incident Response — Incident Response Assistance [J] {Org}
 - 10.5.1.8.6.8 IR-08 Incident Response — Incident Response Plan [J] {Org}
 - 10.5.1.8.6.9 IR-08(1) Incident Response — Incident Response Plan - Breaches [P] {Org}
- 10.5.1.8.7 MP-01 Media Protection — Policy and Procedures [J] {Org}
 - 10.5.1.8.7.1 MP-06 Media Protection — Media Sanitization [J] {Sys}
- 10.5.1.8.8 PE-01 Physical and Environmental Protection — Policy and Procedures [J] {Org}
 - 10.5.1.8.8.1 PE-08(3) Physical and Environmental Protection — Visitor Access Records - Limit Personally Identifiable Information Elements [P] {Sys}
- 10.5.1.8.9 PL-01 Planning — Policy and Procedures [J] {Org}
 - 10.5.1.8.9.1 PL-02 Planning — System Security and Privacy Plan [J] {Hybrid}
 - 10.5.1.8.9.2 PL-04 Planning — Rules of Behavior [J] {Org}
 - 10.5.1.8.9.3 PL-04(1) Planning — Rules of Behavior - Social Media and External Site/Application Usage Restrictions [J] {Org}
 - 10.5.1.8.9.4 PL-08 Planning — Security and Privacy Architecture [J] {Sys}
 - 10.5.1.8.9.5 PL-09 Planning — Central Management [J] {Org}
- 10.5.1.8.10 PM-01 Program Management
 - 10.5.1.8.10.1 PM-03 Program Management — Information Security and Privacy Resources [J] {Org}
 - 10.5.1.8.10.2 PM-04 Program Management — Plan of Action and Milestones (POA&M) Process [J] {Org}
 - 10.5.1.8.10.3 PM-05(1) Program Management — System Inventory - Inventory of Personally Identifiable Information [P] {Org}
 - 10.5.1.8.10.4 PM-06 Program Management — Measures of Performance [J] {Org}
 - 10.5.1.8.10.5 PM-07 Program Management — Enterprise Architecture [J] {Org}
 - 10.5.1.8.10.6 PM-08 Program Management — Critical Infrastructure Plan [J] {Org}
 - 10.5.1.8.10.7 PM-09 Program Management — Risk Management Strategy [J] {Org}
 - 10.5.1.8.10.8 PM-10 Program Management — Authorization Process [J] {Org}
 - 10.5.1.8.10.9 PM-11 Program Management — Mission and Business Process Definition [J] {Org}
 - 10.5.1.8.10.10 PM-13 Program Management — Security and Privacy Workforce [J] {Org}
 - 10.5.1.8.10.11 PM-14 Program Management — Testing, Training, and Monitoring [J] {Org}
 - 10.5.1.8.10.12 PM-15 Program Management — Security and Privacy Groups and Associations [J] {Org}
 - 10.5.1.8.10.13 PM-17 Program Management — Protecting Controlled Unclassified Information on External Systems [J] {Org}

-
- 10.5.1.8.10.14 PM-18 Program Management — Privacy Program Plan [P] {Org}
 - 10.5.1.8.10.15 PM-19 Program Management — Privacy Program Leadership Role [P] {Org}
 - 10.5.1.8.10.16 PM-20 Program Management — Dissemination of Privacy Program Information [P] {Org}
 - 10.5.1.8.10.17 PM-20(1) Program Management — Dissemination of Privacy Program Information - Privacy Policies on Websites, Applications, and Digital Services [P] {Org}
 - 10.5.1.8.10.18 PM-21 Program Management — Accounting of Disclosures [P] {Org}
 - 10.5.1.8.10.19 PM-22 Program Management — Personally Identifiable Information Quality Management [P] {Org}
 - 10.5.1.8.10.20 PM-23 Program Management — Data Governance Body [J] {Org}
 - 10.5.1.8.10.21 PM-24 Program Management — Data Integrity Board [P] {Org}
 - 10.5.1.8.10.22 PM-25 Program Management — Minimization of Personally Identifiable Information Used for Testing, Training, and Research [P] {Org}
 - 10.5.1.8.10.23 PM-26 Program Management — Complaint Management [P] {Org}
 - 10.5.1.8.10.24 PM-27 Program Management — Privacy Reporting [P] {Org}
 - 10.5.1.8.10.25 PM-28 Program Management — Risk Framing [J] {Org}
 - 10.5.1.8.10.26 PM-31 Program Management — Continuous Monitoring Strategy [J] {Org}
 - 10.5.1.8.11 PS-01 Personnel Security — Policy and Procedures [J] {Org}
 - 10.5.1.8.11.1 PS-06 Personnel Security — Access Agreements [J] {Org}
 - 10.5.1.8.12 PT-01 Personally Identifiable Information Processing and Transparency — Policy and Procedures [P] {Org}
 - 10.5.1.8.12.1 PT-02 Personally Identifiable Information Processing and Transparency — Authority to Process Personally Identifiable Information [P] {Org}
 - 10.5.1.8.12.2 PT-03 Personally Identifiable Information Processing and Transparency — Personally Identifiable Information Processing Purposes [P] {Hybrid}
 - 10.5.1.8.12.3 PT-04 Personally Identifiable Information Processing and Transparency — Consent [P] {Hybrid}
 - 10.5.1.8.12.4 PT-05 Personally Identifiable Information Processing and Transparency — Privacy Notice [P] {Hybrid}
 - 10.5.1.8.12.5 PT-05(2) Personally Identifiable Information Processing and Transparency — Privacy Notice - Privacy Act Statements [P] {Hybrid}
 - 10.5.1.8.12.6 PT-06 Personally Identifiable Information Processing and Transparency — System of Records Notice [P] {Org}
 - 10.5.1.8.12.7 PT-06(1) Personally Identifiable Information Processing and Transparency — System of Records Notice - Routine Uses [P] {Org}
 - 10.5.1.8.12.8 PT-06(2) Personally Identifiable Information Processing and Transparency — System of Records Notice - Exemption Rules [P] {Org}
 - 10.5.1.8.12.9 PT-07 Personally Identifiable Information Processing and Transparency — Specific Categories of Personally Identifiable Information [P] {Org}

-
- 10.5.1.8.12.10 PT-07(1) Personally Identifiable Information Processing and Transparency — Specific Categories of Personally Identifiable Information - Social Security Numbers [P] {Hybrid}
 - 10.5.1.8.12.11 PT-07(2) Personally Identifiable Information Processing and Transparency — Specific Categories of Personally Identifiable Information - First Amendment Information [P] {Org}
 - 10.5.1.8.12.12 PT-08 Personally Identifiable Information Processing and Transparency — Computer Matching Agreements [P] {Org}
 - 10.5.1.8.13 RA-01 Risk Assessment — Policy and Procedures [J] {Org}
 - 10.5.1.8.13.1 RA-03 Risk Assessment — Risk Assessment [J] {Sys}
 - 10.5.1.8.13.2 RA-07 Risk Assessment — Risk Response [J] {Sys}
 - 10.5.1.8.13.3 RA-08 Risk Assessment — Privacy Impact Assessments [P] {Hybrid}
 - 10.5.1.8.14 SA-01 System and Services Acquisition — Policy and Procedures [J] {Org}
 - 10.5.1.8.14.1 SA-02 System and Services Acquisition — Allocation of Resources [J] {Org}
 - 10.5.1.8.14.2 SA-03 System and Services Acquisition — System Development Life Cycle [J] {Sys}
 - 10.5.1.8.14.3 SA-04 System and Services Acquisition — Acquisition Process [J] {Sys}
 - 10.5.1.8.14.4 SA-08(33) System and Services Acquisition — Security and Privacy Engineering Principles - Minimization [P] {Sys}
 - 10.5.1.8.14.5 SA-09 System and Services Acquisition — External System Services [J] {Org}
 - 10.5.1.8.14.6 SA-11 System and Services Acquisition — Developer Testing and Evaluation [J] {Sys}
 - 10.5.1.8.15 SC-01 System and Communications Protection — Policy and Procedures [J] {Org}
 - 10.5.1.8.15.1 SC-07(24) Boundary Protection — Personally Identifiable Information [P] {Sys}
 - 10.5.1.8.16 SI-01 System and Information Integrity — Policy and Procedures [J] {Org}
 - 10.5.1.8.16.1 SI-12 System and Information Integrity — Information Management and Retention [J] {Sys}
 - 10.5.1.8.16.2 SI-12(1) System and Information Integrity — Information Management and Retention - Limit Personally Identifiable Information Elements [P] {Sys}
 - 10.5.1.8.16.3 SI-12(2) System and Information Integrity — Information Management and Retention - Minimize Personally Identifiable Information in Testing, Training, and Research [P] {Sys}
 - 10.5.1.8.16.4 SI-12(3) System and Information Integrity — Information Management and Retention - Information Disposal [P] {Sys}
 - 10.5.1.8.16.5 SI-18 System and Information Integrity — Personally Identifiable Information Quality Operations [P] {Sys}
 - 10.5.1.8.16.6 SI-18(4) System and Information Integrity — Personally Identifiable Information Quality Operations - Individual Requests [P] {Sys}
 - 10.5.1.8.16.7 SI-19 System and Information Integrity — De-Identification [P] {Sys}

Exhibits

- 10.5.1-1 Glossary and Acronyms
- 10.5.1-2 References

10.5.1.1

(05-08-2025)

Program Scope and Objectives

- (1) This IRM lays the foundation to:
 - a. Protect the privacy of sensitive but unclassified (SBU) data for taxpayers and personnel, including personally identifiable information (PII), such as federal tax information (FTI, referred to in this IRM as tax information), tax return, financial, and employment information regardless of format.
 - b. Use SBU data (including PII and tax information) throughout the privacy lifecycle (creation, collection, receipt, use, processing, maintenance, access, inspection, display, storage, disclosure, dissemination, or disposal, collectively referred to as processing) only as authorized by law for the purposes collected and as necessary to fulfill IRS responsibilities following the IRS Privacy Principles in IRM 10.5.1.3.2. [National Institute of Standards and Technology (NIST) SP 800-53]

Note: Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining. [NIST SP 800-53 PT-02]

 - c. Destroy or dispose of SBU data when no longer required for business use, in a secure manner to protect privacy.
 - d. Implement and maintain a strong privacy program, which enables the IRS to provide e-government services. Refer to Pub 5499, IRS Privacy Program Plan.
- (2) This IRM covers IRS-wide privacy policy, including:
 - a. Definition of SBU data (including PII and tax information).
 - b. IRS Privacy Principles.
 - c. IRS-wide privacy roles and responsibilities.
 - d. Privacy guidance on topics such as email, telework, and contractors.
 - e. Introduction to privacy-related programs.
- (3) This IRM covers all sensitive data used and operated by and for the IRS no matter what stage of the IT lifecycle (such as production, pre-production, and post-production systems).

10.5.1.1.1

(05-08-2025)

Purpose of the Program

- (1) The PGLD vision is to lead the nation in privacy rights protection. The PGLD mission is to preserve privacy and enhance public trust through proper authentication, access, disclosure, retention, and protection of all data and records.
- (2) The privacy and security of taxpayer and personnel information is one of the IRS's highest priorities. PGLD owns privacy and records management policy and initiatives and coordinates privacy and records management-related actions throughout the IRS. [OMB A-130]
- (3) PGLD is committed to ensuring the protection of SBU data, including taxpayer and personnel PII, from unauthorized access. The organization identifies and reduces threats to privacy and increases awareness of criminal activities aimed at compromising this information. PGLD also leads IRS privacy and records management policies, coordinates privacy protection guidance and activities, responds to privacy complaints, and promotes data protection awareness throughout the IRS. [OMB A-130]
- (4) This IRM defines the uniform policies used by IRS personnel and organizations to carry out privacy-related responsibilities.

- a. To protect SBU data and allow the use, access, and disclosure of information following applicable laws, policies, federal regulations, Office of Management and Budget (OMB) Circulars, Treasury Directives (TDs), National Institute of Standards and Technology (NIST) Publications, other regulatory guidance, and best practice methodologies.
 - b. To use best practices methodologies and frameworks, such as Enterprise Architecture (EA) and One Solution Delivery Life Cycle, (OneSDLC, replaced Enterprise Life Cycle (ELC)), to document and improve IRS privacy policy efficiency and effectiveness.
- (5) This IRM establishes the minimum baseline privacy policy and requirements for all IRS SBU data (including PII and tax information) to:
- a. Establish and maintain a comprehensive privacy program. [OMB A-130]
 - b. Follow privacy requirements and manage privacy risks. [OMB A-130]
 - c. Ensure the protection and proper use of IRS SBU data.
 - d. Prevent unauthorized access to IRS SBU data.
 - e. Enable operation of IRS environments and business units that meet the requirements of this policy and support the business needs of the organization.
- (6) You may use practices that are more restrictive than those defined in this IRM.
- (7) It is the policy of the IRS to protect privacy and safeguard confidential tax information. For more information, review IRM 10.5.1.3.2, IRS Privacy Principles.
- Caution:** Policies continue to apply in exigent circumstances. The IRS will post exceptions through the *internal Interim Guidance site* as needed.
- (8) The Director, PGLD, is the IRS Chief Privacy Officer (CPO). The Director, PPC, is the Bureau Privacy and Civil Liberties Officer (BPCLO). For more information about PGLD, refer to IRM 1.1.27, Privacy, Governmental Liaison and Disclosure (PGLD), and the *internal PGLD Disclosure and Privacy Knowledge Base*.
- (9) Treasury houses the Senior Agency Official for Privacy (SAOP) for the IRS, while the IRS CPO is the executive director responsible for the IRS privacy program.

10.5.1.1.2
(05-08-2025)
Audience

- (1) The audience to which the provisions in this manual apply includes:
- a. All IRS organizations.
 - b. All IRS employees with any access to SBU data (including PII and tax information).
 - c. All IRS personnel, which includes individuals and organizations with contractual arrangements with the IRS, including seasonal or 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 and operated by and for the IRS no matter what stage of the IT lifecycle (such as production, pre-production, and post-production systems).

- (2) For this IRM, IRS personnel or users includes:

- Employees
- Seasonal or temporary employees
- Interns
- Detailees
- Consultants
- IRS contractors (including contractors, subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers)
- Non-person entity (NPE), such as robotic process automation (RPA), bots, artificial intelligence (AI) workers, and digital assistants.

Note: Although these entities are not necessarily capable of following IRS privacy policy, the human parties using them are responsible. These entities must still follow the privacy controls.

- (3) Authorized or Unauthorized personnel applies to whether they are authorized or not authorized to perform an action. To be authorized, all personnel must have a need to know and 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]

10.5.1.1.3
(09-15-2023)
**Policy and Program
Owners**

- (1) Privacy Policy and Knowledge Management (PPKM) under PGLD's Privacy Policy and Compliance (PPC) develops privacy policy following applicable laws, mandates, guidance, mission, and input from other stakeholders. Review Exhibit 10.5.1-2, References.
- (2) For more information about PGLD, refer to IRM 1.1.27, Privacy, Governmental Liaison and Disclosure (PGLD), and the *internal PGLD Disclosure and Privacy Knowledge Base*.

10.5.1.1.4
(12-31-2020)
Primary Stakeholders

- (1) All business units are stakeholders for privacy.

10.5.1.1.5
(05-08-2025)
Background

- (1) This IRM serves as the framework for IRS privacy policy and an introduction to PGLD.
- (2) This policy establishes the privacy context for the development of related subordinate IRMs, IRS publications, and subordinate job aids such as Standard Operating Procedures (SOP).
- (3) Subordinate IRMs offer added privacy program protection information.
- (4) If IRM 10.5.1 conflicts with or varies from the subordinate IRMs in the IRM 10.5 series or guidance, IRM 10.5.1 takes precedence, unless the subordinate IRM is more restrictive or otherwise noted.
- (5) Where this policy cites a subsection, it includes by reference its subsections.

Example: The reference to IRM 10.5.1.6.8, Email and Other Electronic Communications, also includes its six subsections.

- (6) Where this policy uses the term **includes**, it gives examples, not an all-inclusive list. This means the list of items after that does not limit the references to exclude something not listed.
- (7) To deviate from privacy policy, follow the Form 14675, Decision Making Framework Risk Acceptance Form and Tool (RAFT), process in consultation with the CPO. [OMB A-130, TD P 85-01] The executive or other senior official with the authority to formally assume responsibility for the process must sign the RAFT as the approver. The RAFT clearly documents business decisions in the context of risk appetite and acceptance. Send the RAFT to PPKM for review for compliance with privacy laws and regulations. PPKM will not grant exceptions to bypass laws or mandates. Send RAFT review requests via email to **Privacy* (give topic name in subject line and add Attn: CPO RAFT review). For *RAFT guidance*, refer to the *internal Office of the Chief Risk Officer site*.
- (8) This policy assigns responsibilities and lays the foundation necessary to measure privacy progress and compliance.

10.5.1.1.6
(05-08-2025)
Authority

- (1) PGLD's Privacy Policy and Knowledge Management (PPKM) implements relevant privacy statutes, regulations, guidelines, OMB Memoranda, and other requirements. Various statutes, such as the Privacy Act, Federal Information Security Modernization Act (FISMA), and Paperwork Reduction Act mandate compliance with OMB policy and NIST guidance, giving them the force of law.
- (2) 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 are responsible for being familiar with and acting in accord with taxpayer rights. Refer to IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For more information about the TBOR, refer to *Taxpayer Bill of Rights (external)*. The TBOR requires the IRS to protect taxpayer rights to privacy and confidentiality.
- (3) To reference the origin of a privacy policy cited later in this IRM (such as a law, OMB, NIST, or Treasury), this IRM may reference a requirement's origin in brackets at the end of the guidance, such as [Strict Confidentiality] (IRS Privacy Principles), [AC-01] (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.
- (4) For a full list of authority references, review Exhibit 10.5.1-2, References.
- (5) The primary laws include:
 - Privacy Act
 - Computer Matching and Privacy Protection Act
 - Freedom of Information Act (FOIA)
 - Internal Revenue Code (IRC, primarily 26 USC 6103, also known as IRC 6103, and 26 USC 7803(a)(3), also known as IRC 7803(a)(3))
 - The Taxpayer Browsing Protection Act
 - Federal Information Security Modernization Act of 2014 (FISMA)
 - E-Government Act
- (6) The most relevant OMB circulars and memos include:

- OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
 - OMB Circular No. A-130, Management of Federal Information Resources
 - M-03-22 – OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
 - M-10-22 – Guidance for Online Use of Web Measurement and Customization Technologies
 - M-10-23 – Guidance for Agency Use of Third-Party Websites and Applications
 - M-16-24 – Role and Designation of Senior Agency Officials for Privacy
 - M-17-12 – Preparing for and Responding to a Breach of Personally Identifiable Information
 - M-23-22 – Delivering a Digital-First Public Experience
- (7) Relevant NIST guidance includes:
- NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
 - NIST SP 800-63, Digital Identity Guidelines
 - NIST SP 800-88, Guidelines for Media Sanitization
 - NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
 - NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- (8) Relevant Department of the Treasury directives and publications include:
- Treasury Directive Publication (TD P) 15-71, Treasury Security Manual
 - Treasury's Privacy and Civil Liberties Impact Assessment (PCLIA) Template and Guidance
 - TD P 85-01, Treasury Information Technology (IT) Security Program
- (9) 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 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]
- (10) Primary authorities for processing PII include:
- *5 USC (external)*, Government Organization and Employees, primarily section 301
 - *18 USC (external)*, Crimes and Criminal Procedure, primarily section 1030
 - *26 USC (external)*, Internal Revenue Code, primarily sections 6001, 6011, 6012, 6109, 7801
 - *31 USC (external)*, Money and Finance, primarily section 330
- (11) IRS Policy Statements 1-1 and 10-2 support these authorities in:
- IRM 1.2.1.2.1, Policy Statement 1-1, Mission of the Service.
 - IRM 1.2.1.17.2, Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safeguarding Confidential Tax Information.

10.5.1.1.7
(09-15-2023)

Roles and Responsibilities

- (1) Review IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities.

10.5.1.1.8
(09-15-2023)

Program Management and Review

- (1) Business units hold responsibility for managing their program and showing how effectiveness and objectives are measured within the scope of this IRM.
- (2) For PGLD program management and review, the IRS formally documents its privacy program in Pub 5499, IRS Privacy Program Plan.
- (3) The NIST technical security and privacy controls address federal IT systems.

10.5.1.1.9
(09-15-2023)

Program Controls

- (1) Business units hold responsibility for showing and documenting the program controls developed to oversee their program as well as ensuring employee compliance with all applicable elements of this IRM.
- (2) For PGLD program controls, the IRS formally documents its privacy program in Pub 5499, IRS Privacy Program Plan.
- (3) The NIST technical security and privacy controls address federal IT systems. For all the controls relevant to privacy, review IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls.

10.5.1.1.10
(09-15-2023)

Terms and Acronyms

- (1) Review Exhibit 10.5.1-1, Glossary and Acronyms.

10.5.1.1.11
(09-15-2023)

Related Resources

- (1) Review Exhibit 10.5.1-2, References.

10.5.1.2
(03-23-2018)

Key Privacy Definitions

- (1) To support the IRS mission, understanding the key privacy definitions in the following subsections is essential.

10.5.1.2.1
(05-08-2025)

Privacy Lifecycle

- (1) The concept of a privacy and information lifecycle refers to 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. [OMB A-130]

Note: Per NIST, processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining. [NIST SP 800-53 PT-02]

- (2) IRS personnel must protect SBU data (including PII and tax information) throughout the privacy lifecycle, from receipt to disposal.
- (3) This IRM uses the term processing to refer to all the steps in the privacy lifecycle.

10.5.1.2.2
(05-08-2025)
**Sensitive But
Unclassified (SBU) Data**

- (1) Sensitive but unclassified (SBU) data is any information which if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations), or the privacy to which individuals are entitled under the Privacy Act. For the full definition, refer to TD P 15-71, Treasury Security Manual, Chapter III, Section 24, Sensitive But Unclassified Information.
- (2) SBU data includes:
 - a. Tax information (also known as federal tax information, FTI, protected by IRC 6103), personally identifiable information (PII), protected health information (PHI), certain procurement information, system vulnerabilities, case selection methodologies, system information, enforcement procedures, and investigation information. Review IRM 10.5.1.2.2.1, Examples and Categories of SBU Data.
 - b. Live data, which is production data in use. Live means that when changing the data, it changes in production. Authorized personnel may extract the data (such as for testing or development), but then it is no longer "live." Live data often is SBU data (including PII and tax information), but tax information stays tax information whether *live* in a production environment or removed to a non-production environment.

Note: For Classified National Security Information (CNSI), refer to IRM 10.9.1, Classified National Security Information, for procedures for protecting CNSI.
- (3) All IRS personnel must protect SBU data. Personnel must restrict access, inspection, and disclosure of SBU data to others who have a need to know the information. This restriction applies to SBU data the IRS processes and makes available to taxpayers and other outside parties. IRS personnel must remove access from non-IRS personnel when the need no longer exists. Review IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data. [Strict Confidentiality]
 - a. For more information on encryption and other protections, review IRM 10.5.1.6, Practical Privacy Policy.
 - b. For more information on the need to know, review IRM 10.5.1.2.8, Need To Know.
 - c. Refer to IRM 10.8.1.4.1.5, AC-06 Least Privilege (InTC), for information about limiting access to people who have a need to know the information.
 - d. Refer to IRM 11.3.22.2.1, Access by IRS Employees.
- (4) SBU data includes categories of protected information which many IRS personnel handle daily, such as PII and tax information. It also includes other categories, such as procurement (which can include general procurement and acquisition, small business research and technology, and source selection) and system information (which can include critical infrastructure categories like information systems vulnerability information, physical security, and emergency management).
- (5) Personnel must decide if the SBU data is necessary to do business (does it support the business purpose of the system or the organization's mission?). If it does not serve a valid business purpose, then the IRS must not collect that SBU data. If that SBU data does serve a business purpose, then the IRS may use it throughout the privacy lifecycle properly. For more information, review IRM 10.5.1.3.2, IRS Privacy Principles. [Privacy Act; Purpose Limitation; Minimizing Collection, Use, Retention, and Disclosure]

- (6) All IRS personnel must identify and mark SBU data as such following IRM 10.5.1.6.5, Marking. SBU data so marked is not meant for public release. [TD P 15-71]
- (7) SBU data in a public record is still SBU data, but different protections apply. To decide if publicly available SBU data or SBU data in the public record is still sensitive, review IRM 10.5.1.2.3.2, Public Record.
- (8) Constitutionally required disclosures: Some situations require disclosure of information, including SBU data, such as criminal cases where the IRS has a constitutional obligation to disclose, upon the defendant's request, evidence material either to guilt or punishment (exculpatory evidence). For more details, refer to IRM 11.3.35, Requests and Demands for Testimony and Production of Documents.
- (9) Complete a Qualifying Questionnaire for any system using SBU data to decide when it has PII and needs a Privacy and Civil Liberties Impact Assessment (PCLIA). Refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA). [RA-08]
- (10) For more information on PII, review IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII.

10.5.1.2.2.1 (05-08-2025)

Examples and Categories of SBU Data

- (1) Some examples and categories of IRS SBU data include, as outlined in the tables in this subsection:
 - a. Tax information (FTI)
 - b. Privacy (PII)
 - c. SBU data and its other categories, such as procurement, finance, law enforcement, critical infrastructure, and legal
- (2) While SBU data is the overarching term for all IRS sensitive data, we use categories to highlight the sensitivity of the data. If information falls into more than one category, we categorize it based on its source. If related to a tax account, categorize it as FTI (even if it is also PII or SBU data). If it identifies an individual, but not FTI, categorize it as PII (mostly personnel information). If it is sensitive, but not FTI or PII, categorize it as SBU data.
- (3) This table lists some examples of the tax information (FTI) category of SBU data.

SBU Data Category	Example
Tax information, FTI	FTI, which includes individual and corporate (or other business) tax return information under IRC 6103.
Tax information, FTI	Tax convention.
Tax information, FTI	Taxpayer Advocate information.
Tax information, FTI	Written determinations.

- (4) This table lists some examples of the privacy (PII) category of SBU data.

Note: If related to a tax account, this is also tax information or FTI. You may mark it as FTI to highlight its sensitivity to meet the SBU data marking requirement in IRM 10.5.1.6.5, Marking.

SBU Data Category	Example
Privacy, PII	Death records. If related to a tax account, this is tax information or FTI.
Privacy, PII	General privacy (includes Privacy Act). If related to a tax account, this is tax information or FTI.
Privacy, PII	Genetic information.
Privacy, PII	Health information, also known as protected health information (PHI). If related to a tax account, this is tax information or FTI.
Privacy, PII	Personnel records (includes Privacy Act and 5 CFR 293.106).
Privacy, PII	Student records. If related to a tax account, this is tax information or FTI.

(5) This table lists some examples of other categories of SBU data.

Note: If related to a tax account, this is also tax information or FTI. If it identifies an individual, but is not related to a tax account, this is also PII. You may mark it as FTI or PII, respectively, to highlight its sensitivity to meet the SBU data marking requirement in IRM 10.5.1.6.5, Marking.

SBU Data Category	Example
SBU	Documents marked Official Use Only (OUO).
SBU	Case selection methodologies including tolerance criteria or general investigation parameters.
SBU	Proprietary processes or algorithms used in investigative work or tax processing.
SBU	Proprietary business information entrusted to the IRS. If related to a tax account, this is tax information or FTI.
SBU	Confidential data to be released to the public later.
SBU	18 USC 1905 information protected under the Trade Secrets Act (trade secrets, processes, operations, style of work, or apparatus, or confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association). If related to a tax account, this is tax information or FTI.
SBU, Critical infrastructure	Information system vulnerabilities information (referred to as system information in this IRM), which includes passwords.
SBU, Critical infrastructure	Physical security information, such as details of facility vulnerabilities (such as entry codes or badge access).
SBU, Critical infrastructure	Emergency management.

SBU Data Category	Example
SBU, Finance	Bank Secrecy Act (31 USC Bank Secrecy Act protected reports filed by financial institutions). Sometimes called extremely sensitive SBU data. If related to a tax account, this is tax information or FTI.
SBU, Finance	Budget.
SBU, Finance	Electronic funds transfer. If related to a tax account, this is tax information or FTI.
SBU, Finance	General financial information. If related to a tax account, this is tax information or FTI.
SBU, Law enforcement	General law enforcement (procedures and training materials).
SBU, Law enforcement	Informant (identification, activities, contacts, payments, and correspondence). Sometimes called extremely sensitive SBU data. If related to a tax account, this is tax information or FTI.
SBU, Law enforcement	Investigation (identifiers, associations, and relationships; investigative records received from other law enforcement and regulatory agencies, foreign and domestic; records related to investigation related travel and financing). If related to a tax account, this is tax information or FTI.
SBU, Law enforcement	Law enforcement financial records (and other records obtained via witness consent, subpoena, summons, search warrant, or any other legal process). If related to a tax account, this is tax information or FTI.
SBU, Law enforcement	Pen register or trap and trace.
SBU, Law enforcement	Reward (recipient and payment information).
SBU, Law enforcement	Whistleblower identity. Refer to IRC 7623 or the Whistleblower Protection Act of 1989, Pub.L. 101-12 as amended, and IRM 25.2.1, General Operating Division Guidance for Working Whistleblower Claims). Sometimes called extremely sensitive SBU data.
SBU, Legal	Administrative proceedings.
SBU, Legal	Collective bargaining.
SBU, Legal	Federal Grand Jury (18 USC Grand Jury information protected by Rule 6(e) of the Federal Rules of Criminal Procedure). Sometimes called extremely sensitive SBU data. If related to a tax account, this is tax information or FTI.
SBU, Legal	Legal privilege (including draft, pre-decisional, and deliberative information).
SBU, Legal	Legislative materials (including Congressional or state).
SBU, Procurement	General procurement and acquisition (such as contract proposals).
SBU, Procurement	Small business research and technology.
SBU, Procurement	Source selection.

10.5.1.2.2.2
(05-08-2025)
**Official Use Only and
Limited Official Use**

- (1) Documents previously designated as **Official Use Only** (OUO) and **Limited Official Use** (LOU) include SBU data. Treasury policy requires using SBU data to describe such documents. [TD P 15-71]

Exception: Per IRM 1.11.2.5.3, Designate IRM Content as Official Use Only (OUO), the publishing process uses OUO for marking sensitive material and may continue this practice until the IRS implements the Controlled Unclassified Information (CUI) program. Once implemented, CUI marking requirements will override OUO and SBU data marking requirements. For more information on CUI, refer to the *internal Controlled Unclassified Information site*.

- (2) For more information, refer to IRM 11.3.12, Designation of Documents.

10.5.1.2.2.3
(09-24-2020)
**Freedom of Information
Act (FOIA) and SBU
Data**

- (1) The Freedom of Information Act (FOIA) exempts most SBU data from release to the public under one of the nine exemptions listed in 5 USC 552(b).
- (2) The fact that the IRS must release certain information if requested under FOIA does not automatically remove its status as SBU data. [FOIA]
- (3) For more information, refer to IRM 11.3.13, Freedom of Information Act.

10.5.1.2.3
(05-08-2025)
**Personally Identifiable
Information (PII)**

- (1) Personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. [OMB A-130]
- (2) For IRS purposes:
 - a. To *distinguish* an individual is to identify an individual. For example, an individual might be distinguished by a passport identification number or Social Security Number (SSN). However, a list of credit scores without any other information concerning the individual does not distinguish the individual.
 - b. To *trace* an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status, such as with an audit log.
 - c. *Linked* information is information about or related to an individual that is logically associated with other information about the individual.
 - d. *Linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. [GAO Report 08-536 (*external*), Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008]
- (3) Information **permitting the physical or online contacting of a specific individual** [E-Government Act section 208(b)(1)(A)(ii)(II)] is the same as **information in identifiable form**, [OMB M-03-22] which means that it is PII.
- (4) The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.
- (5) Non-PII can become PII when more information becomes available — in any medium and from any source — that, when combined with other available in-

formation, could be used to identify an individual. [NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII); OMB M-10-23]

- (6) Review IRM 10.5.1.2.3.1, Examples and Categories of PII, for more information.
- (7) PII is SBU data. You may mark it as PII to meet the SBU data marking requirement in IRM 10.5.1.6.5, Marking.
- (8) If PII is related to a tax account, it is also tax information or FTI. If PII is also tax information, you may mark it as FTI to highlight its sensitivity to meet the SBU data marking requirement in IRM 10.5.1.6.5, Marking.
- (9) Privacy Act information is PII, but not all PII is a Privacy Act record. Review IRM 10.5.1.2.7, Privacy Act Information.
- (10) Submit a PCLIA for any system using PII. Refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA). [RA-08]
- (11) PII in a public record is still PII, but different protections apply. To decide if publicly available PII or PII in the public record is still sensitive, review IRM 10.5.1.2.3.2, Public Record.
- (12) You must protect PII as you do any SBU data. For more information on PII, review IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII.

10.5.1.2.3.1
(05-08-2025)
Examples and
Categories of PII

- (1) Examples and categories of PII may include the following, when used to distinguish or trace an individual's identity, or when combined with information that is linked or linkable to an individual:

Note: If related to a tax account, this is also tax information (FTI). You may mark it as FTI to highlight its sensitivity to meet the SBU data marking requirement in IRM 10.5.1.6.5, Marking.

Data Category	Examples and categories of PII
Privacy, PII	Name, such as: <ul style="list-style-type: none">• Full name• Birth name• Mother's birth name• Alias• Name control (first 4 letters of last name)
Privacy, PII	Address information, such as street address or email address.

Data Category	Examples and categories of PII
Privacy, PII	<p>A unique set of numbers or characters assigned to a specific individual, such as:</p> <ul style="list-style-type: none"> • Telephone numbers, including mobile, business, and personal numbers • SSN or ITIN, including the last 4 digits • Taxpayer identification number (TIN) that identifies an individual, such as an employer identification number (EIN) for a sole proprietorship or partnership • Document locator number (DLN) to identify an individual's record • Email or internet protocol (IP) address • Driver's license number • Passport number • Financial account or credit card number • Standard employee identifier (SEID) • Automated Integrated Fingerprint Identification System (AIFIS) identifier, booking, or detention system number • Universally unique identifier (UUID), a unique random number generated for each individual taxpayer in the electronic authentication process • Any other kind of identification number or card, including state ID or alien card ID
Privacy, PII	<p>Employee and employee information, including personnel records, employment testing materials, medical information, information concerning reasonable accommodations for disabilities, claims, and litigation. [Privacy Act; 5 CFR 293]</p> <p>Note: For privacy protections for pandemics and employee illness, refer to Infectious Disease in the Workplace, Document 13001. For more about the application of the Privacy Act in this situation, refer to IRM 10.5.6.2.4, Health or Safety Disclosure. For further privacy protections on disability and reasonable accommodation information, refer to IRM 1.20.2.4, Confidentiality and Disclosure.</p>
Privacy, PII	<p>Individual tax return information, including adjusted gross income (AGI) or combinations of fields that identify an individual. Review IRM 10.5.1.2.4, Federal Tax Information (FTI).</p>
Privacy, PII	<p>Corporate or other business tax return information that identifies an individual, such as an S-Corporation, partnership, or sole proprietorship.</p>
Privacy, PII	<p>Personal data, including:</p> <ul style="list-style-type: none"> • Date of birth • Place of birth • Age • Religious affiliation • Sexual orientation • Gang affiliation • Behavior patterns

Data Category	Examples and categories of PII
Privacy, PII	Personal characteristics, including: <ul style="list-style-type: none"> • Height • Weight • Sex • Hair color • Eye color • Race • Ethnicity • Scars • Tattoos • Distinguishing features • Photographic image (especially of face or other distinguishing characteristic) • Biometric information (such as x-rays, fingerprints, retina scan, voice, facial geometry) • Genetic information
Privacy, PII	Asset information, such as media access control (MAC) address, device ID, or other host-specific persistent static identifier that consistently links to a person or small, well-defined group of people.
Privacy, PII	Descriptions of events or times (information in documents, such as behavior patterns, incident and data breach reports, police reports, arrest reports, and medical records).
Privacy, PII	Descriptions of locations, such as geographic information system (GIS), Global Positioning System (GPS) data, and electronic bracelet monitoring information.
Privacy, PII	Information identifying personally owned property, such as vehicle registration number or title number and related information.
Privacy, PII	Information about an individual that is linked or linkable to one of the above.
Privacy, PII	Death records. If related to a tax account, this is tax information or FTI.
Privacy, PII	Health information, also known as protected health information (PHI). If related to a tax account, this is tax information or FTI.
Privacy, PII	Student records.

10.5.1.2.3.2
(05-08-2025)
Public Record

- (1) IRS personnel must protect SBU data regardless of whether the same information is in the public record or publicly available, but less stringent protections might apply in some situations.
- (2) Personnel must encrypt SBU data (including PII), but inside the IRS network, encryption is not required if the IRS proactively makes it available to all personnel on internal resource sites (including Discovery Directory, Outlook™ [calendar, profile information, and address book], and SharePoint™ or Teams™ site collections), such as names, SEID, and business contact information. [NIST SP 800-122; TD P 85-01, Appendix A, AC-20(3)_T.028, and MP-06(3)_T.124]
- (3) Email addresses, by themselves as the method of the email conveyance, do not need encrypting, but when combined with the content and attachments of an email, the email address may become SBU data.

- a. Encryption rules still apply for the body of emails and attachments.
 - b. Review IRM 10.5.1.6.8, Email and Other Electronic Communications, for more information on email.
- (4) As for other SBU data and PII in the public record or publicly available, the requirements differ, depending on the information.
- Note:** Tax information always requires protection under IRC 6103. Review IRM 10.5.1.2.4, Federal Tax Information (FTI).
- (5) No IRC 6103 public records exemption exists, but IRM 11.3.11.12, Information Which Has Become Public Record, discusses disclosure of matters that have become public records, such as court cases. This is known as the judicially created public records exception.
- (6) Treasury security guidance exempts Treasury information made available proactively to the public from certain encryption controls. This exemption implies a public records exception for information the agency makes available to the public. [TD P 85-01, Appendix A, AC-20(3)_T.028, and MP-06(3)_T.124]
- (7) The Public Information Listing (PIL) from OPM makes certain federal employee information available to the public by FOIA request. For more information, refer to IRM 11.3.13.7.3.1, Public Information Listing. [5 CFR 293.311]
- (8) IRS policy also authorizes the withholding of the public information items of employees in certain cybersecurity positions, not identified by a specific series or position title.
- (9) Exercise caution and consult with PGLD for any questions they might have about application of a public record exception, on a case-by-case basis, before reducing privacy protections based on a public record exception. For further information, email **Privacy*.
- (10) For more information, refer to IRM 11.3.13, Freedom of Information Act.

10.5.1.2.3.3 (05-08-2025) Defining PII versus Sensitive PII

- (1) Little difference exists between PII and what personnel refer to as “sensitive” PII. For the definition of PII, review IRM 10.5.1.2.3, Personally Identifiable Information (PII).
- (2) The level of risk and sensitivity increases with the potential level of harm caused by exposed SBU data or PII.
- (3) Context is important. PII that does not seem high risk or sensitive may still require protection if its context makes it risky or sensitive. For example, a collection of names in a list, file, or query:

Is sensitive PII if...	Is <i>not</i> sensitive PII if ...
Individual taxpayers who filed returns.	Attendees at a public meeting.
Employees with poor performance ratings.	Names out of a public telephone book.
Employee emergency contact information.	Names of SharePoint site members.
Law enforcement personnel.	FOIA listing of IRS employees in non-protected positions.

10.5.1.2.4
(05-08-2025)
**Federal Tax Information
(FTI)**

- (4) For more information, review IRM 10.5.1.6.1.1, Deciding Risk Levels for SBU Data and PII.
- (1) The term tax information, or federal tax information (FTI), refers to a taxpayer's return and return information protected from unauthorized disclosure under IRC 6103. This law defines return information as any information the IRS has about a tax or information return, liability, or potential liability under Title 26. This return information includes a taxpayer's:
 - a. Identity.
 - b. Income, payments, deductions, exemptions, or credits.
 - c. Assets, liabilities, or net worth.
 - d. Tax liability investigation status (whether the IRS ever investigates or examines the return).
- (2) Redacting, masking, or truncating tax information does not change its nature. It is still tax information.
- (3) Tax information in IRS business processes comes under many names, such as FTI, IRC 6103 protected information, 6103, taxpayer data, taxpayer information, tax return information, return information, case information, SBU data, and PII. Do not use the term "live data" to describe tax information, unless in a production environment as discussed in IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data.
- (4) Tax information is SBU data. IRC 6103 protects tax information from unauthorized disclosure. When tax information relates to an individual, that SBU data is also PII. [IRC 6103(b)(2)]
- (5) You may mark tax information as FTI to meet the SBU data marking requirement in IRM 10.5.1.6.5, Marking.
- (6) You must protect tax information as you do any SBU data. Review IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data.
- (7) Submit a PCLIA for any system using tax information. Refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA). [RA-08]
- (8) Review these subsections in this IRM for more information:
 - IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII.
 - IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data.
 - IRM 10.5.1.2.3, Personally Identifiable Information (PII).
- (9) For more information about return information and a definition, refer to IRM 11.3.1.4, Disclosure and Safeguarding of Returns and Return Information.

10.5.1.2.5
(12-31-2020)
UNAX

- (1) The term UNAX defines the act of committing an unauthorized access or inspection of any tax information contained on paper or within any electronic format. An access or inspection is unauthorized if done without a management-assigned IRS business need.
- (2) The IRS created the unauthorized access or inspection of tax information and records (UNAX) program to implement privacy protection and statutory unauthorized access and browsing prevention requirements.

- (3) The Taxpayer Browsing Protection Act defines UNAX. For more information about UNAX, refer to the *internal UNAX site* and IRM 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance, and Requirements.

10.5.1.2.6
(12-31-2020)
**Unauthorized Access of
SBU Data**

- (1) While statutory UNAX (based on the Taxpayer Browsing Protection Act) refers to unauthorized access to tax information, other statutes, Treasury, and IRS policy govern unauthorized access to SBU data. [TD P 15-71, Treasury Security Manual, Chapter III, Section 24, Sensitive But Unclassified Information]
- (2) The term unauthorized access of SBU data defines the act of committing an unauthorized access or inspection of any SBU data (not tax information) contained on paper or within any electronic format. An access or inspection is unauthorized if done without a management-assigned IRS business need.
- (3) Review IRM 10.5.1.2.2, Sensitive but Unclassified (SBU) Data, and IRM 10.5.1.2.8, Need To Know.
- (4) Refer to 18 U.S. Code 1030 - Fraud and related activity in connection with computers; 44 USC 3551-3558; and the Privacy Act.

10.5.1.2.7
(05-08-2025)
Privacy Act Information

- (1) The Privacy Act forms the core of IRS privacy policy. It provides certain safeguards for an individual against an invasion of personal privacy by requiring federal agencies to:
 - a. Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that ensures that such action is for a necessary and lawful purpose.
 - b. Ensure that the information is current and accurate.
 - c. Ensure that the information is for its intended use.
 - d. Provide adequate safeguards.
- (2) The Privacy Act applies to agency records retrieved by an identifier for an individual who is a US citizen or an alien permanently admitted to US residence. A group of these records is a system of records (SOR).
- (3) The term "record" includes education, financial transactions, medical history, and criminal or employment history, and that has name, or the identifying number, symbol, or other identifying element assigned to the individual, such as a fingerprint or a photograph.
- (4) Responsible IRS personnel must publish a System of Records Notice (SORN) in the Federal Register when establishing a new system of records, **before** retrieving the information by an identifier.
- (5) Privacy Act information is PII because it identifies individuals. That means it is also SBU data. As with any other SBU data, you must allow disclosure only to persons authorized to have access to the information under to the Privacy Act.

Note: Not all PII is Privacy Act information.

- (6) Personnel records are Privacy Act information when retrieved by an identifier. Refer to IRM 10.5.6.8, Personnel Records.

10.5.1.2.8
(05-08-2025)
Need To Know

- (7) For more information on the conditions of disclosure, refer to IRM 10.5.6.2.2, Conditions of Disclosure Under the Privacy Act.

- (1) Restrict access to SBU data (including PII and tax information) to those IRS personnel who have a need for the information in the performance of their duties.
- (2) The term “need to know” describes the requirement that personnel may access SBU data (including PII and tax information) only as authorized to meet a legitimate business need, which means personnel need the information to perform official duties. Review examples later in this subsection for explanations of how need to know applies to duties.

Note: Review IRM 10.5.1.2.6, Unauthorized Access of SBU Data, and IRM 10.5.1.2.5, UNAX.

- (3) Personnel (including current employees, rehired annuitants, and returning contractors) who change roles or assignments may access only the SBU data (including PII and tax information) for which they still have a business need to know to perform their duties. When you no longer have a business need to know, you must not access the information. This policy includes information in systems, files (electronic and paper), and emails, even if technology does not prevent access.

Example: A compliance case has a litigation hold or similar request in place. Even if in a new assignment, you may keep and access old case files from your earlier role if you need to retrieve them for a litigation hold or similar request.

Example: A former employee now works for a vendor who has a contract with the IRS. The former employee must not access old files in email or on their laptop from their earlier role with the IRS, even if archived under their SEID. The IRS will supply any information necessary to perform the current contract on a need-to-know basis.

Example: You search for something on SharePoint™, and the result shows you a file with sensitive information that doesn't relate to your duties. Even though technology access controls failed and showed you information you don't have a need to know, you must not look at the information. Report this inadvertent unauthorized access following UNAX or disclosure responsibilities in IRM 10.5.1.4.1, Employees and Personnel.

Note: To decide applicability of employee duties, based on sensitivity of information, refer to the position description or contact Labor Relations.

- (4) You must make sure you follow this need-to-know policy.
- (5) This standard is less stringent than a “cannot function without it” test. For each use, consider whether you need the information to perform official duties properly or efficiently. Necessary for official duties in this context does not mean essential or indispensable, but proper and helpful in obtaining the information sought.

- (6) Management must inform personnel who have a need to know of the protection requirements under the law and make sure they have the proper level of clearance through a background investigation, typically covered by the onboarding and training process.
- (7) Need to know supports the “relevant and necessary” aspect of the Purpose Limitation Privacy Principle and the Privacy Act. It conveys the statutory restrictions to disclose protected information to those who have an authorized need for the information in the performance of their duties. The Strict Confidentiality Privacy Principle requires this, as does the NIST Privacy Control for Privacy Monitoring and Auditing and Security Controls in the Access Control family. [Purpose Limitation; Strict Confidentiality; Privacy Act; IRC 6103 and 7803(a)(3); UNAX; Treasury’s Privacy and Civil Liberties Impact Assessment (PCLIA) Template and Guidance; NIST SP 800-53]
- (8) Access to CNSI requires more stringent controls outlined in IRM 10.9.1, Classified National Security Information.
- (9) Refer to IRM 11.3.22.2.1, Access by IRS Employees.

10.5.1.2.9
(09-15-2023)
Authentication

- (1) Authentication is the process of establishing or confirming that someone is the previously identified person they claim to be. For authentication policy, refer to IRM 10.10.3, Centralized Authentication Policy – Centralizing Identity Proofing for Authentication Across All IRS Channels.
- (2) Authentication makes sure that the individual is who they claim to be but says nothing about the access rights of the individual. For more information about authentication technical security controls, refer to IRM 10.8.1, Security Policy.

10.5.1.2.10
(05-08-2025)
Authorization

- (1) Authorization refers to both the legal authority (such as IRC 6103) and the organizational authority for processing data. For more information about tax information authorization, refer to IRM 11.3.1.2, Disclosure Code, Authority, and Procedure (CAP).
- (2) To be authorized, all personnel must have a need to know and 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]
- (3) External authorization is the process that verifies that external parties have the legal rights or privileges to interact with the IRS on behalf of themselves or others (such as other government agencies, businesses, or individuals). Such authority might be by a formal request for information processed using established written procedures, a memorandum of understanding, or an executed agreement.
- (4) Authorization is required for any person or business conducting IRS business on another person’s behalf (such as tax return preparers).
- (5) IT authorization covers access privileges granted to a user, program, or process or the act of granting those privileges. Refer to the term **authorization** in IRM 10.8.1, Security Policy.

10.5.1.2.11
(05-08-2025)
High Security Items

- (1) High security items are original or certified paper documents with SBU data (including PII and tax information), typically received and processed in IRS office controlled or limited areas, that management must not allow personnel to remove from the facility. These are **highly sensitive documents** in IRM 6.800.2.2.8, Denial of Telework Agreement Requests. Refer to IRM 10.2.14.3, Protecting Assets.

Exception: This policy does not apply to field employees whose positions allow them to have such documents in a field environment (such as Criminal Investigation Special Agents and field compliance Revenue Agents and Revenue Officers). Those positions have more controls and requirements to protect and to process such documents promptly (for example, refer to IRM Parts 5 and 9). For more information about field work, review IRM 10.5.1.6.9.1, Field and Travel, and IRM 10.5.1.6.9, Other Forms of Transmission.

- a. Examples of such high security items include certain original federal records, original tax returns and related original correspondence, payments, original legal documents (such as affidavits), and primary identification documents (such as drivers' licenses, passports, birth certificates, and Social Security cards).

Example: Payments and original paper tax returns received in campus controlled or limited areas.

Note: Properly manage original paper federal records generated by IRS personnel outside the office, even on telework, the same as you would in the office. Refer to the *internal Telework Privacy Considerations site* for more information.

- b. The IRS office controlled or limited areas include large amounts (or in highly concentrated and easily alterable or destroyable form) of highly sensitive information requiring protection. Refer to IRM 10.2.14.3.5, Security Areas.
- c. Do not take high security items to a telework location. You may use electronic or paper copies of high security items, if the originals remain in the office's secured environment. Review IRM 10.5.1.6.12, Telework. Refer to IRM 6.800.2.2.8, Denial of Telework Agreement Requests.

- (2) Send questions about high security items to the **Privacy* mailbox.

10.5.1.3
(09-15-2023)
Key Privacy Concepts

- (1) The IRS Privacy Principles and federally mandated privacy controls from NIST describe how the IRS protects an individual's right to privacy.
- (2) Following the IRS Privacy Principles and privacy controls is mandatory for management officials responsible for protecting SBU data (including PII and tax information).

10.5.1.3.1
(05-08-2025)
Privacy Controls

- (1) OMB A-130 mandates federal agencies implement NIST security and privacy controls.
- (2) The IRS formally documents its privacy program in Pub 5499, IRS Privacy Program Plan.
- (3) These privacy and security controls are the technical controls that address

federal IT systems. For all the controls relevant to privacy, review IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls.

- (4) The subsection IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls, is for technical management officials developing and supporting IT systems, including management, senior management and executives, system owners, system developers, and authorizing officials. For more information about these roles, refer to IRM 10.8.2.3, IT Security Roles and Responsibilities.
- (5) The NIST Special Publication (SP) 800-53 Revision 5 (Rev 5) controls establish a relationship between privacy and security controls. Per Section 2.4, Security and Privacy Controls:

The selection and implementation of security and privacy controls reflect the objectives of information security and privacy programs and how those programs manage their respective risks. Depending on the circumstances, these objectives and risks can be independent or overlapping. Federal information security programs are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (such as unauthorized activity or system behavior) to provide confidentiality, integrity, and availability. Those programs are also responsible for managing security risk and for ensuring compliance with applicable security requirements. Federal privacy programs are responsible for managing risks to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal (collectively referred to as “processing”) of personally identifiable information (PII) and for ensuring compliance with applicable privacy requirements. When a system processes PII, the information security program and the privacy program have a shared responsibility for managing the security risks for the PII in the system. Due to this overlap in responsibilities, the controls that organizations select to manage these security risks will generally be the same regardless of their designation as security or privacy controls in control baselines or program or system plans.

10.5.1.3.2 (05-08-2025) **IRS Privacy Principles**

- (1) The public trusts the IRS and its personnel to protect their privacy and safeguard their confidential information.
- (2) The IRS is dedicated to meeting this expectation. You must act in a way that shows a commitment to treat individuals fairly, honestly, and respectfully, and always protect their right to privacy. [OMB A-130]
- (3) Protecting privacy and safeguarding confidential information is a public trust. To keep this trust, the IRS and its personnel must follow these privacy principles:
 1. Accountability
 2. Purpose Limitation
 3. Minimizing Collection, Use, Retention, and Disclosure
 4. Openness and Consent
 5. Strict Confidentiality
 6. Security
 7. Data Quality
 8. Verification and Notification
 9. Access, Correction, and Redress
 10. Privacy Awareness and Training

- (4) The IRS derived the privacy principles from the Fair Information Practice Principles (FIPPs) and the Privacy Act. The Privacy Act requires that information be relevant, accurate, necessary, and timely (RANT).
- (5) 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 are responsible for being familiar with and acting in accord with taxpayer rights. Refer to IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For more information about the TBOR, refer to *Taxpayer Bill of Rights (external)*. The TBOR requires the IRS to protect taxpayer rights to privacy (with due process) and confidentiality as essential rights that help protect their civil liberties.
- (6) IRS Policy Statements 1-1 and 10-2 highlight these principles in:
 - IRM 1.2.1.2.1, Policy Statement 1-1, Mission of the Service.
 - IRM 1.2.1.17.2, Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safeguarding Confidential Tax Information.
- (7) The IRS Privacy Principles form an overarching privacy ethical framework for the IRS to apply to SBU data (including PII and tax information). Use of this framework promotes the integrity and trustworthiness the public expects and deserves.
- (8) For a poster of the IRS Privacy Principles, refer to Document 14540, IRS Privacy Roadmap. For more details on each of the privacy ethical principles, refer to the *internal IRS Privacy Principles site*.

10.5.1.3.2.1
(09-15-2023)
Accountability

- (1) All IRS personnel are responsible and accountable for the effective implementation of privacy protections.
- (2) Privacy is personal. Do what's right with sensitive information. Treat it like it's your own. Put privacy first.

10.5.1.3.2.2
(09-15-2023)
Purpose Limitation

- (1) Use or collect PII only when necessary and relevant for legitimate IRS purposes, namely tax administration and other authorized purposes.
- (2) Privacy is a public trust. Limit using data to the purpose collected, for what is relevant and necessary for a legitimate IRS purpose. Don't sell sensitive data.

10.5.1.3.2.3
(05-08-2025)
Minimizing Collection, Use, Retention, and Disclosure

- (1) Limit the collection, use, retention, and disclosure of PII to what is minimally necessary for the specific purposes for which the IRS collected it, unless specifically authorized.
- (2) Privacy is simplicity. Data minimization means to access and use only the sensitive information you need. Just because you can access and collect data doesn't mean you should. Reduce clutter. Keep it only if you must. Dispose of and manage it properly.

10.5.1.3.2.4
(09-15-2023)
Openness and Consent

- (1) The IRS makes its privacy policies and practices readily available to individuals, such that we inform individuals of the collection, use, retention, and disclosure of their PII, and we get individuals' consent to the greatest extent practical.

Note: Consent can be explicit (verbal or by other action) or implied (by continuing or inaction).

- (2) Privacy is transparency. Tell individuals what we do with their information and why we need it, so they know what to expect. Get consent to collect data.

10.5.1.3.2.5
(09-15-2023)
Strict Confidentiality

- (1) Only access or disclose PII to authorized individuals who require the information for the performance of official duties. The IRS does not tolerate browsing of confidential information, including PII and tax information, by unauthorized IRS personnel. Protected information includes confidential information of all individuals, not just taxpayers. Protected information includes confidential information of IRS employees, volunteers, practitioners, and other individuals who interact with the IRS.
- (2) Privacy is discretion. Keep sensitive information private. Don't talk about your cases. Share data only with those who have a need to know.

10.5.1.3.2.6
(09-15-2023)
Security

- (1) Provide appropriate administrative, technical, and physical safeguards to protect against the unauthorized collection, use, and disclosure of SBU data, including PII and tax information.
- (2) Privacy is protection. Safeguard sensitive information. You can't have privacy without security.

10.5.1.3.2.7
(09-15-2023)
Data Quality

- (1) Follow requirements governing the accuracy, completeness, and timeliness of PII to ensure fair treatment of all individuals. Collect information, to the greatest extent practical, directly from the individual to whom it relates.
- (2) Privacy is fairness. Be fair. Go to the source for sensitive information. Data is no good if it's wrong.

10.5.1.3.2.8
(09-15-2023)
Verification and Notification

- (1) Verify all information about an individual with the individual, as well as any other relevant sources, to the greatest extent possible before taking adverse action based on that information. Notify individuals before final action to the greatest extent possible.
- (2) Privacy is assurance. Verify information and provide individuals with prompt notification before acting.

10.5.1.3.2.9
(05-08-2025)
Access, Correction, and Redress

- (1) Allow individuals to access and correct their PII upon request to the greatest extent allowable. Individuals include taxpayers, IRS employees, IRS contractors, practitioners, and others who interact with the IRS. Individuals will be able to contest determinations made based on allegedly incomplete, inaccurate, or out-of-date PII to the greatest extent allowable.
- (2) Privacy is visibility. Allow individuals to access their own information when allowable. Make it right.

10.5.1.3.2.10
(09-15-2023)
Privacy Awareness and Training

- (1) Make IRS personnel aware of the proper treatment of SBU data, including PII and tax information, and train them accordingly.
- (2) Privacy is fundamental. Learn what you need to know about privacy. Be aware of how to protect data.

10.5.1.4
(09-15-2023)

IRS-Wide Privacy Roles and Responsibilities

- (1) The IRS implements privacy roles and responsibilities for personnel following federal laws and privacy guidelines.
- (2) These subsections list responsibilities for:
 - a. IRM 10.5.1.4.1, Employees and Personnel
 - b. IRM 10.5.1.4.2, Management
 - c. IRM 10.5.1.4.3, Senior Management and Executives
 - d. IRM 10.5.1.4.4, System Owners
 - e. IRM 10.5.1.4.5, System Developers
 - f. IRM 10.5.1.4.6, Authorizing Officials
 - g. IRM 10.5.1.4.7, Personnel in Contract Activities
- (3) For the role of the Chief Privacy Officer (CPO), refer to IRM 1.1.27.1.4, Roles and Responsibilities.

10.5.1.4.1
(05-08-2025)

Employees and Personnel

- (1) IRS personnel (as defined in IRM 10.5.1.1.2, Audience) must follow the responsibilities in paragraphs (2) through (14).
- (2) Keep informed of and follow applicable IRS privacy policies and procedures, including the IRS Privacy Principles in IRM 10.5.1.3.2. This means carrying out the mission of the IRS, which requires the IRS to safeguard privacy and protect privacy rights. Review the IRS Privacy Principle in IRM 10.5.1.3.2.1, Accountability.
- (3) Limit access to records that include SBU data only to those authorized individuals with a need to know. You are always responsible for the information you share. Review the IRS Privacy Principles in IRM 10.5.1.3.2.3, Minimizing Collection, Use, Retention, and Disclosure, and IRM 10.5.1.3.2.5, Strict Confidentiality.
- (4) Use SBU data only for the purposes for which the IRS collected it. Review the IRS Privacy Principle in IRM 10.5.1.3.2.2, Purpose Limitation.
- (5) Limit the use and disclosure of SBU data to that which is necessary and relevant for tax administration and other legally mandated or authorized purposes. Review the IRS Privacy Principle in IRM 10.5.1.3.2.2, Purpose Limitation.
- (6) Prevent unnecessary access, inspection, and disclosure of SBU data in information systems, programs, electronic formats, and hardcopy documents by following proper safeguarding measures. Review the IRS Privacy Principles in IRM 10.5.1.3.2.5, Strict Confidentiality, and IRM 10.5.1.3.2.6, Security.
- (7) Safeguard IRS information and information systems entrusted to them. Review the IRS Privacy Principle in IRM 10.5.1.3.2.6, Security.
- (8) Use IRS email accounts for performance of official duties. Review the IRS Privacy Principle in IRM 10.5.1.3.2.1, Accountability.
- (9) Follow existing IT Security Policy and IRS System Security Rules (the IRS Rules of Behavior in the *internal Business Entitlement Access Request System (BEARS)*) on use of IRS-furnished equipment to process IRS information, not personally-owned or non-IRS furnished equipment (including cloud or web-based systems or services). These IRS Rules of Behavior serve as the **rules of conduct** required by the Privacy Act section (e)(9). Refer to IRM 10.8.1.4.1.19.1, Personally-Owned and Other Non-Government Furnished Equipment.

Review the IRS Privacy Principle in IRM 10.5.1.3.2.6, Security. [PL-4; PS-06]

- (10) Complete IRS annual and role-based privacy, information protection, and disclosure training requirements, UNAX awareness briefings, records management awareness briefing, and all other specialized privacy training, as required. Review the IRS Privacy Principle in IRM 10.5.1.3.2.10, Privacy Awareness and Training.

Note: To be authorized, all personnel must have a need to know and 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]

- (11) Immediately complete Form 11377-E, Taxpayer Data Access, to document the access of tax information when direct case assignment does not support the access, the access was in error, or when the access may raise a suspicion of an unauthorized access. Review the IRS Privacy Principles in IRM 10.5.1.3.2.5, Strict Confidentiality, and IRM 10.5.1.3.2.6, Security.
- (12) Stay aware of the consequences of UNAX violations, including accessing your own records, those of coworkers, family, friends, celebrities, and other covered relationships. For information about the IRS-wide UNAX program and links to all UNAX forms, refer to the *internal UNAX site*. Review the IRS Privacy Principles in IRM 10.5.1.3.2.5, Strict Confidentiality, and IRM 10.5.1.3.2.6, Security.
- (13) Report incidents and data breaches immediately upon discovery to:
- Your manager and
 - The proper organizations based on what was lost, stolen, destroyed, or disclosed.

Note: For more information on reporting an incident and data breaches, refer to IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures, or the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.

Review the IRS Privacy Principles in IRM 10.5.1.3.2.5, Strict Confidentiality, and IRM 10.5.1.3.2.6, Security.

- (14) Follow privacy and security responsibilities outlined in IRM 10.8.1, Security Policy, and IRM 10.8.2, IT Security Roles and Responsibilities. Review the IRS Privacy Principle in IRM 10.5.1.3.2.6, Security.

10.5.1.4.2 (05-08-2025) Management

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employees and Personnel, management must follow the responsibilities in paragraphs (2) through (10).
- (2) Communicate IRS privacy policies and procedures clearly to all personnel in your organizations, ensuring awareness of their responsibilities to protect SBU data (including PII and tax information) and uphold applicable privacy laws, regulations, and IRS policies and procedures.
- (3) Make sure personnel with authorized access to SBU data receive training to carry out their roles and responsibilities consistent with IRS privacy policies. [OMB A-130]

- (4) Make sure all personnel in their respective organizations follow the IRS privacy policies and procedures. Also address any noncompliance and remedy it promptly, including, if necessary, the initiation of penalties for noncompliance following federal law and IRS personnel rules and regulations.
- (5) Prevent UNAX violations proactively in your respective areas. Make sure all personnel are trained and knowledgeable of the Taxpayer Browsing Protection Act of 1997, the consequences of UNAX violations for personnel, and that all personnel within their business area complete all IRS UNAX, privacy, information protection, and disclosure training requirements annually and as required for their position.

Note: To be authorized, all personnel must have a need to know and 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]

- (6) Make sure personnel use proper safeguards to prevent unintentional exposure to SSNs in cases where SSN use is necessary.
- (7) Use the SEID as the primary employee identifier as an alternative use for SSNs when possible.
- (8) Make sure personnel promptly complete PCLIAAs for which you are the responsible official. Mitigate any privacy risks discovered. The IRS requires PCLIAAs for pilot projects, research, experimentation, the use of innovative technologies, technical demonstrations, prototypes, and proof of concepts, and the like. For more information about the PCLIA process, refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA), and IRM 2.31.1.4.4, OneSDLC Product Cycle Compliance Process. [RA-08]
- (9) Follow IRS records management requirements outlined in the IRM 1.15 series, Records and Information Management.
- (10) Make sure all personnel report incidents and data breaches immediately upon discovery to:
 - Your manager and
 - The proper organizations based on what was lost, stolen, destroyed, or disclosed.

Note: For more information on reporting an incident and data breach, refer to IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures, or the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.

10.5.1.4.3
(12-31-2020)

**Senior Management and
Executives**

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employees and Personnel, and IRM 10.5.1.4.2, Management, senior management and executives must also follow the responsibilities in paragraphs (2) through (7).

- (2) Coordinate with the Chief Privacy Officer (CPO) to develop, implement, maintain, and enforce a program to protect all SBU data (including PII and tax information) for which they are responsible following IRS privacy policies and procedures. [OMB A-130]
- (3) Focus special emphasis on the government-wide requirements to eliminate the unnecessary collection and use of SSNs as a personal identifier for employee and tax systems and programs. [OMB A-130]
- (4) Periodically assess and evaluate privacy awareness activities of your organization to set clear expectations for compliance with all requirements.
- (5) Allocate sufficient resources to follow IRS privacy policies and procedures. [OMB A-130]
- (6) Make sure the IRS uses alternative unique identifiers for internal and taxpayer systems and programs in place of SSNs when possible.
- (7) To deviate from privacy policy, follow the Risk Acceptance Form and Tool (RAFT) process in consultation with the CPO. [OMB A-130, TD P 85-01] For details, review IRM 10.5.1.1.5 (7), Background.

10.5.1.4.4
(05-08-2025)
System Owners

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employees and Personnel, IRM 10.5.1.4.2, Management, and IRM 10.5.1.4.3, Senior Management and Executives, IRS IT system owners must follow the responsibilities in paragraphs (2) through (15).
- (2) Integrate information security and privacy fully into the system development process. [OMB A-130] This means to include privacy at the table for planning and discussion.
- (3) Follow applicable laws, regulations, and IRS privacy policies and procedures in the development, acquisition, implementation, operation, and disposal of all systems under their control. Follow the OneSDLC process. For more information about OneSDLC, refer to IRM 2.31.1, One Solution Delivery Life Cycle Guidance, or the *OneSDLC site*.
- (4) Follow the NIST SP 800-53 Security and Privacy Controls as cited in IRM 10.5.1.8 and IRM 10.8.1.
- (5) Limit the use of SBU data (including PII and tax information) throughout the privacy lifecycle to that which is minimally necessary for tax administration purposes or other legally authorized purposes.
- (6) Examine the use of SSNs in all information systems and programs, as well as hardcopy and electronic formats (for example, forms, printouts, screenshots, displays, electronic media, archives, and online storage repositories) and eliminate the unnecessary use of SSNs where identified.
- (7) Use adequate SSN alternatives, as necessary.
- (8) Make sure, where possible, that the IRS uses SBU data that is relevant, accurate, necessary, and timely (RANT).
- (9) Make sure that all new systems, systems under development, or systems undergoing major modifications with SBU data have in place a completed and approved PCLIA following federal laws and IRS policy, including the NIST SP

800-53 privacy controls. The IRS requires PCLIAAs for pilot projects, research, experimentation, the use of innovative technologies, technical demonstrations, prototypes, and proof of concepts, and the like. [RA-08]

- (10) Work with Privacy Compliance and Assurance (PCA) to review approved PCLIAAs to redact SBU data or PII from the PCLIA before posted to IRS.gov.
- (11) Coordinate with the system developer and PCA to document privacy risks identified on the PCLIA or privacy controls assessment in their Plans of Action and Milestones (POA&Ms) and to resolve them promptly.
- (12) Coordinate all inter-agency PII sharing agreements with PGLD's Governmental Liaison, Disclosure, and Safeguards (GLDS) and other affected IRS entities that establish and monitor the sharing of PII with external entities.
- (13) Implement safeguards to establish and monitor internal and third-party agreements for SBU data protection and confidentiality.
- (14) Make sure that IRS personnel involved in the management, operation, programming, maintenance, or use of IRS information systems complete IRS UNAX and privacy, information protection and disclosure training before being granted access to those systems that include SBU data.
- (15) Make sure that IRS personnel who have access to SBU data for testing follow the requirements of IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments. For more information, refer to the *internal SBU Data Use Process site*.

10.5.1.4.5
(05-08-2025)
System Developers

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employees and Personnel, and IRM 10.5.1.4.2, Management, system developers must follow the responsibilities in paragraphs (2) through (9).
- (2) Integrate information security and privacy fully into the system development process. [OMB A-130] This means to include privacy at the table for planning and discussion.
- (3) Follow IRS privacy policies and procedures in the development, implementation, and operation of information systems for which they are responsible. Follow the OneSDLC process. For more information about OneSDLC, refer to IRM 2.31.1, One Solution Delivery Life Cycle Guidance, or the *OneSDLC site*.
- (4) Work with system owners to eliminate the unnecessary accessing, collecting, displaying, sharing, transferring, keeping, and using of SSNs in all IRS systems, especially personnel and tax systems.
- (5) Develop information systems that provide the ability to partially mask, truncate, or redact the SSN when the total elimination of the use of SSNs is not possible in both personnel and tax systems.
- (6) Establish, maintain, and test the management, operational, and technical controls to protect SBU data (including PII and tax information).
- (7) Complete system PCLIAAs working with system owners and following IRS policy, if they are the responsible management official or designees. The IRS requires PCLIAAs for pilot projects, research, experimentation, the use of innovative technologies, technical demonstrations, prototypes, and proof of concepts, and the like. [RA-08]

- (8) Coordinate with the system owners and PCA to resolve identified privacy risks and POA&Ms.
- (9) Perform system lifecycle reviews to ensure satisfactory resolution of privacy risks and give the results to the system owners.

10.5.1.4.6
(05-08-2025)
Authorizing Officials

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employees and Personnel, and IRM 10.5.1.4.2, Management, the authorizing official (AO) (refer to IRM 10.8.2.3.1.7, Authorizing Official) must follow the responsibilities in paragraphs (2) through (3).
- (2) Develop and maintain operational documentation (such as action and implementation plans, standard operating procedures) necessary for implementation of the privacy controls, outlined in the IRM 10.5 series, Privacy and Information Protection.
- (3) Implement privacy requirements, including documentation and procedures for managing, administering, and monitoring their information systems. For more information about this role, refer to IRM 10.8.2.3.1.7, Authorizing Official (AO).

10.5.1.4.7
(05-08-2025)
Personnel in Contract Activities

- (1) In addition to the Employees and Personnel responsibilities in IRM 10.5.1.4.1, IRS contracting officers (COs), contracting officer's representatives (CORs), and other personnel engaged in contract-related activities must follow the requirements in the subsections outlined in the following table, if they apply to their respective roles [Privacy Act, IRC 6103(n), OMB A-130]:

Note: In this policy, contracts and contract-related activities include terms like procurements, acquisitions, requests for proposals, solicitations, performance work statements, task orders, statement of objectives, pilot projects, research, experimentation, the use of innovative technologies, technical demonstrations, prototypes, and proof of concepts (referred to here collectively as contracts).

IRM	Title
IRM 10.5.1.6.15	Contracts
IRM 10.5.1.6.15.1	Contract Privacy Requirements Language
IRM 10.5.1.6.15.2	Contracting Officer's Representative (COR) Training
IRM 10.5.1.6.15.3	OneSDLC in Contracts
IRM 10.5.1.6.15.4	Privacy Act in Contracts
IRM 10.5.1.6.15.5	IRC 6103 (Tax Information) in Contracts
IRM 10.5.1.6.15.6	Background Investigation
IRM 10.5.1.6.15.7	Mandatory Training for Contractors
IRM 10.5.1.6.15.8	Non-Disclosure Agreements
IRM 10.5.1.6.15.9	Privacy and Security Controls in Contracts

IRM	Title
IRM 10.5.1.6.15.10	Privacy and Civil Liberties Impact Assessment (PCLIA) in Contracts
IRM 10.5.1.6.15.11	Testing and Development Environments in Contracts
IRM 10.5.1.6.15.12	Incident Response in Contracts
IRM 10.5.1.6.15.13	Unauthorized Access (UNAX) in Contracts
IRM 10.5.1.6.15.14	Contract Closeout
IRM 10.5.1.6.15.15	Federal Acquisition Regulation (FAR) Compliance
IRM 10.5.1.8.9.2	PL-4 Planning – Rules of Behavior [J] {Org}
IRM 10.5.1.8.10.13	PM-17 Program Management – Protecting Controlled Unclassified Information on External Systems [J] {Org}
IRM 10.8.1.4.14.1	PS-02 Position Risk Designation
IRM 10.8.1.4.14.2	PS-03 Personnel Screening (InTC)
IRM 10.5.1.8.11.1	PS-6 Personnel Security – Access Agreements [J] {Org}
IRM 10.5.1.8.14.3	SA-04 System and Services Acquisition – Acquisition Process [J] {Sys}

- (2) Contract privacy requirements apply to contractors, subcontractors, contractor employees, and subcontractor employees. Contract requirements flow down to subcontracts (which the IRS must approve) under the *internal IRS Acquisition Policy (IRSAP) site Index C (pdf)*.
- (3) For more procurement information, refer to *internal Office of the Chief Procurement Officer Customer Portal*.
- (4) For more privacy information, refer to the *internal contracts site*.
- (5) For help with these responsibilities, email **Privacy*.

10.5.1.5 (12-31-2020) Privacy Culture

- (1) The IRS requires a privacy culture, where all personnel think about privacy before acting. In such an environment or culture, protecting privacy guides the day-to-day practices and routines of everyone.
 - (2) Throughout the privacy lifecycle, consider whether the use of SBU data (including PII and tax information) meets all the IRS Privacy Principles.
- Note:** One approach might be to ask if you would want your information treated in this way.
- (3) The IRS has programs to promote a privacy culture.

10.5.1.5.1
(05-08-2025)
Clean Desk Policy

- (1) The IRS has a clean desk policy. To protect SBU data (including PII and tax information) when not in your possession, you must lock it up. The clean desk policy requirements apply to data left out in work areas (including those in telework and offsite locations) and non-secured containers, on credenzas, desktops, printers, fax or copy machines, conference rooms, and in or out baskets. [TD P 15-71; Accountability, Strict Confidentiality, Security]
- (2) The clean desk policy also applies to online meetings. Keep a clean desk(top): apply the clean desk policy to your computer screen and anything in view of your camera. Close all applications and documents that don't apply to your call. Review IRM 10.5.1.6.18.2, Online Meetings.
- (3) IRS personnel must containerize all SBU data (including PII and tax information) in non-secured areas during non-duty hours.
- (4) Lock protected data in containers in areas where non-IRS personnel have access during non-duty hours or when not under the direct control of an authorized IRS employee. For more information, refer to IRM 10.2.14.3, Protecting Assets.
- (5) For some pipeline activities and processing conducted at Submission Processing centers, campuses, and computing centers, the volume of the tax information processed and the disruption to these operations might prevent containerization and Clean Desk implementation. We require Clean Desk Waivers for these areas. Submission Processing activity may complete one waiver request for each campus, computing center, or other POD, but we will not grant blanket waivers for any entire facility. Clean Desk Waiver requests must be:
 - a. Restricted to pipeline activities and processing conducted at Submission Processing centers, campuses, and computing centers.
 - b. Justified and not just a matter of convenience.
 - c. Limited to items not requiring special security (SP). Refer to IRM 10.2.14.3, Protecting Assets.
 - d. Supported with a layered security plan that allows the campuses and the computing centers a higher level of protection to accommodate the processing operation.
 - e. Approved at the Executive level of the business unit making the request via Form 14617, Clean Desk Waiver Guidance & Checklist.
 - f. Sent by the business unit to PGLD for approval via email to **Privacy Review*. Facilities Management and Security Services (FMSS) will conduct the physical onsite reviews, with help from PGLD Records Management as necessary.
 - g. Reviewed and approved by FMSS and PGLD, including exemptions citing *voluminous files*.
 - h. Submitted annually, unless no longer required.

10.5.1.5.2
(07-08-2021)
Privacy in Practice (PiP)

- (1) IRS Privacy in Practice includes protecting privacy in systems and safeguarding privacy in everyday business practices. All IRS activities include an element of privacy. A culture of privacy prevails through privacy in practice; from systems development to customer service, training, communications, passwords, and the clean desk policy.
- (2) PGLD Privacy Policy and Compliance (PPC) employees serve as privacy advocates and consultants for IRS personnel and projects.

- (3) Designing privacy into projects is a key aspect of effective privacy policy and compliance at the IRS.
 - a. This concept shows the principle that organizations best achieve privacy goals when they weave privacy proactively into business processes and operational practices.
 - b. To be effective, introduce privacy principles early in a project lifecycle, in architecture planning, system design, contract review and selection, and the development of operational procedures.
- (4) Invite privacy employees when necessary at all project stages to include privacy at the table for planning and discussion. [OMB A-130]
- (5) Refer to Privacy in Practice Quick Reference Guide (Document 13291).
- (6) For help or more information, email **Privacy*.
- (7) Refer to the *internal Enterprise Architecture site*.

10.5.1.6
(12-31-2020)
Practical Privacy Policy

- (1) These subsections describe privacy policy in terms of common issue areas. Many of these areas interrelate with each other, physical protection, and IT security practices.
- (2) For more information, refer to the *internal PGLD Disclosure and Privacy Knowledge Base*.
- (3) For help, email **Privacy*.

10.5.1.6.1
(05-08-2025)
Protecting and Safeguarding SBU Data

- (1) Regardless of the risk, IRS personnel must protect and safeguard SBU data (including PII and tax information). This means you must properly use SBU data throughout the privacy lifecycle.
- (2) You are always responsible for the information you share.
- (3) The requirements in this subsection mirror the IRS-Wide Privacy Roles and Responsibilities in IRM 10.5.1.4 and stem from TD P 15-71, Treasury Security Manual, Chapter III, Section 24, Sensitive But Unclassified Information.
- (4) Be aware of and follow safeguarding requirements for SBU data. Disclosing or accessing SBU data without proper authority could result in administrative or disciplinary action (including termination of contract). The lack of an SBU data marking does not mean the information is not sensitive nor does it relieve you from responsibility to properly safeguard the information from unauthorized use or inadvertent disclosure.
- (5) Take steps to prevent the possibility of such disclosure by non-IRS personnel. Deny access to unauthorized non-IRS personnel in areas not used for serving the public.
- (6) Follow the IRS clean desk policy in IRM 10.5.1.5.1.
- (7) Decide how long to protect the information, for example, either by date or lapse of a determinable event, following the IRM 1.15 series, Records and Information Management.

- (8) IRS security officials must provide routine oversight of measures in place to protect SBU data through a program of routine administration and day-to-day management of their information security program.
- (9) IRS supervisors and program managers hold responsibility for training personnel to recognize and safeguard SBU data supporting their mission, operations, and assets. Supervisors and managers must also make sure affected personnel keep an adequate level of education and awareness. Education and awareness must begin upon initial personnel assignment and be reinforced annually through mandatory training, staff meetings, or other methods contributing to an informed workforce.
- (10) IRS personnel must protect SBU data supporting their mission, operations, and assets. Protection efforts must focus on preventing unauthorized or inadvertent disclosure, especially when visitors enter areas where we process SBU data. This includes being aware of surreptitious and accidental threats posed by high-end communications technologies carried or used by personnel and visitors, such as cell phones (with or without photographic capability), personal data assistants or digital assistants, smart devices, Internet of Things (IoT), portable or pocket computers, cameras, and other video imaging recorders, flash drives, multi-functional, and two-way pagers, and wireless devices capable of storing, processing, or sending information.
- (11) IRS program managers and contracting officials must also require proper privacy and security contract requirements language for personnel, facilities, and information protection through the acquisition process of contracts or grants that concern access to SBU data.

10.5.1.6.1.1
(05-08-2025)

**Deciding Risk Levels for
SBU Data**

- (1) The IRS considers SBU data (including PII and tax information) at a moderate to high risk confidentiality level.
- (2) Loss, compromise, or disclosure of SBU data (including PII and tax information) could result in serious or significant (not limited or minor) harm, embarrassment, inconvenience, or unfairness to an individual (or their privacy) or the IRS.
- (3) Harm includes any adverse effects experienced by an individual whose PII was compromised, or adverse effects to the IRS such as a loss of public confidence.
- (4) The greater the potential for harm, the more at risk the SBU data becomes. As outlined in NIST SP 800-122:

- a. Low confidentiality level means limited potential harm with minor impact on an individual or the IRS.

Example: Low confidentiality level data might include information that the IRS may release under FOIA requests, or information that has become public record or is publicly available. For more information, review IRM 10.5.1.2.2.3, FOIA and SBU Data, and IRM 10.5.1.2.3.2, Public Record.

- b. PII with moderate or high confidentiality levels means the potential harm ranges from serious to severe or catastrophic, with significant to severe impact to an individual or the IRS. Tax information is an example of moderate to high risk PII confidentiality levels.

- (5) The greater the risk to SBU data, the stronger the privacy and security protections become. [OMB A-130, NIST SP 800-122] For example, moderate and high risk SBU data require encryption, but publicly available low risk data might not need encryption. Review IRM 10.5.1.6.2, Encryption.
- (6) When in doubt about the level of risk of SBU data (including PII and tax information), or the privacy concerns around the data, email **Privacy* for help.
- (7) For more information about publicly available information, review IRM 10.5.1.2.3.2, Public Record.
- (8) For more information on the IT aspects of data security, refer to IRM 10.8.1, Security Policy.

10.5.1.6.1.2
(05-08-2025)

Limiting Sharing of SBU Data

- (1) We must protect all SBU data (including PII and tax information). Limit what SBU data we share based on:
 - Authentication (review IRM 10.5.1.2.9, Authentication).
 - Authorization (review IRM 10.5.1.2.10, Authorization).
 - Need to know (review IRM 10.5.1.2.8, Need To Know).

[Purpose Limitation, Strict Confidentiality]
- (2) Share SBU data (orally, visually, or electronically) in a way that avoids access by unauthorized persons. Precautions might include preventing visual access and restricting oral disclosure to authorized individuals.
- (3) You may reproduce SBU data only to the extent needed to carry out official duties. Properly destroy flawed or otherwise unusable reproductions. Review IRM 10.5.1.6.10, Disposition and Destruction.
- (4) The electronic transmission of SBU data (including PII and tax information) requires encryption for security purposes. Review IRM 10.5.1.6.2, Encryption, and IRM 10.5.1.6.9.7, Electronic and Online, for more information.
- (5) The confidentiality provisions of IRC 6103 restrict release of tax information (whether of an individual or business). Share tax information only with authorized individuals following established written procedures. For tax information, follow extensive Disclosure rules in the IRM 11.3 series, Disclosure of Official Information. Removing identifying information (such as name or TIN) from specific tax records does not remove it from the confidentiality protections of IRC 6103.
- (6) For sharing non-tax Privacy Act information (personnel PII), follow IRM 10.5.6.2.2, Conditions of Disclosure under the Privacy Act.
- (7) **Internally:** Only share SBU data (including PII and tax information) with other IRS personnel if the recipient's need for the information is related to their official duties.
- (8) **Externally:** Only share SBU data (including PII and tax information) with authorized individuals outside of IRS, in encrypted files, if you meet all these conditions:
 - a. Individual authorized to receive it under law or regulation, such as the Privacy Act or IRC 6103. Show authority by a formal request for informa-

tion processed using established written procedures, or a memorandum of understanding or executed agreement which also shows the secure method of transmission for the data.

Note: Keep agreements in an approved database or program, such as IRS Agreement Database (IAD). For more information about the IAD, review IRM 10.5.1.7.12, Governmental Liaison (GL).

- b. Recipient need for the information related to official duties.
- c. Recipient authenticated.
- d. Recipient accepted information and any obligation to protect.
- e. Access controls limited to those with need to know.
- f. The applicable System of Records Notice (SORN) includes the use as a published routine use. Refer to the *internal System of Records site* and IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs).

- (9) Refer to the IRM 11.3 series, Disclosure of Official Information, or email **Disclosure* for more guidance.

10.5.1.6.1.3 (09-15-2023) Extracting SBU Data

- (1) IRS personnel must not create unauthorized, unnecessary, or duplicative hardcopy or electronic collections of SBU data (including PII and tax information), such as duplicate, ancillary, shadow, personal copies, or “under the radar” files. [Minimizing Collection, Use, Retention, and Disclosure]
- (2) If creating new spreadsheets or databases that include SBU data (including PII and tax information) from a larger file or database is necessary, consider whether it requires a PCLIA. [RA-08]
 - a. To do so, send a Qualifying Questionnaire (QQ) or Privacy Threshold Assessment (PTA), or email **Privacy*.
 - b. For more information on the QQ, PTA, and PCLIA processes, refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA).

10.5.1.6.1.4 (05-08-2025) Synthetic or Fictitious Data

- (1) Where possible in testing or training or research, use synthetic, fictitious, or masked data. [Minimizing Collection, Use, Retention, and Disclosure; SI-12(2), SI-19]
- (2) Redacting, masking, or truncating tax information does not change its nature. It is still tax information.

Note: Changing a few characters is not enough to protect the data.

- (3) Review IRM 10.5.1.6.19, Training; IRM 10.5.1.8.16.3, System and Information Integrity — Information Management and Retention - Minimize Personally Identifiable Information in Testing, Training, and Research; and IRM 10.5.1.8.16.7, System and Information Integrity — De-Identification.
- (4) For SBU data in non-production environments, refer to IRM 10.5.8.3, SBU Data Process.
- (5) For more resources about fictionalizing or creating fictitious data, refer to Document 13324, Guidelines and Examples for Fictionalizing Domestic Taxpayer Information; Document 13311, International Name and Address Construction Job Aid; IRM 6.410.1.3.10, Disclosure Requirements; and IRM 1.11.2.5.6, Fictitious Identifying Information.

10.5.1.6.2
(05-08-2025)
Encryption

- (1) The IRS uses its IT-approved encryption as a crucial tool to protect SBU data (including PII and tax information). [OMB A-130, TD P 85-01, Security, SC-08, SC-13, SI-03]
- (2) Protect all SBU data (including PII and tax information) with IT-approved encryption methods and access controls, limiting access only to approved personnel with a need to know. This includes SBU data in email, removable media (such as USB drives), on mobile computing devices, and on computers and mobile devices.

Note: The IRS restricts the ability to save data on removable media storage devices. Refer to IRM 10.8.1.4.10, MP-01 Media Protection Policy and Procedures, and *internal removable media guidance (doc)*.

- (3) For IT policy on email encryption, refer to IRM 10.8.1.4.19.2.1, Electronic Mail (Email) Security (and related interim guidance).
- (4) For more details about emailing and encrypting SBU data, review IRM 10.5.1.6.8, Email and Other Electronic Communications.
- (5) Different policies apply for emails to taxpayers and representatives, other stakeholders, those with IRS accounts, and personal email. For more information about emailing outside the IRS, review the following subsections:
 - IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives
 - IRM 10.5.1.6.8.2, Emails to Other External Stakeholders
 - IRM 10.5.1.6.8.3, Emails to IRS Accounts
 - IRM 10.5.1.6.8.4, Emails with Personal Accounts
- (6) Refer to the *internal Encryption site* for encryption instructions.
- (7) Refer to specific requirements in these IRMs:
 - IRM 1.15 series, Records and Information Management.
 - IRM 10.2 series, Physical Security Program.
 - IRM 10.8.1.4.18.12, SC-13 Cryptographic Protection.

10.5.1.6.3
(05-08-2025)
Computers and Mobile Computing Devices

- (1) Protect SBU data (including PII and tax information) on a computer (such as a server, desktop, or mobile computing device [such as a laptop, tablet, or smartphone]). Lock the device (such as with a screen saver), secure it physically, and keep it within sight or control.
- (2) IRS personnel must use encryption, access controls, and physical security measures proper for the equipment and setting.
 - a. For example, computers on IRS sites (federal facilities, contractor's offices, or rented areas) must follow the proper security policies or contractual requirements.
 - b. IRS personnel must not use mobile devices in public settings in such a way as to expose SBU data (including PII and tax information).
 - c. To the extent possible, position any computer or device screen displaying IRS SBU data (including PII and tax information) so that non-authorized personnel cannot view the data.
- (3) Protect equipment. Securely lock computers (such as a server, desktop, or mobile computing device [such as a laptop, tablet, or smartphone]) or other

equipment (such as flash drives, CDs, external drives) when left unattended, whether in the office, in the home, or in a hotel room. Use the IRS-provided cables and cable locks to secure laptops when working in regular workspace (workspace), working out of the office, or in travel status. This policy applies even to personnel who live alone. Always secure equipment.

- (4) For more information about secured wireless access points (wi-fi hotspots), review IRM 10.5.1.6.12, Telework, and refer to IRM 10.8.1.4.1.17, AC-18 Wireless Access.

10.5.1.6.4
(12-31-2020)
Data Loss

- (1) IRS personnel must prevent SBU data loss throughout the privacy lifecycle.
- (2) If such a loss occurs:

Immediately upon discovery of an inadvertent unauthorized disclosure of sensitive information, or the loss or theft of an IT asset or hardcopy record or document that includes sensitive information, you must report the incident and data breach to your manager and the proper organizations based on what was lost or disclosed. [OMB A-130]

- (3) For a brief description of the Incident Management program, review IRM 10.5.1.7.16, Incident Management.
- (4) For more information about how to report an incident and data breach, refer to IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures, or the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.

10.5.1.6.5
(05-08-2025)
Marking

- (1) The Treasury Security Manual [TD P 15-71, Treasury Security Manual, Chapter III, Section 24, Sensitive But Unclassified Information] requires distinct labeling of SBU data (including PII and tax information) to highlight its sensitivity. The lack of SBU data markings does not relieve the holder from safeguarding responsibilities.

Exception: The marking policy does not apply to PII that the IRS proactively makes available to all employees on resource sites (including Discovery Directory, Outlook™ (calendar, profile information [including profile photos], and address book), and SharePoint™ or Teams™ site collections [including profile photos]), such as names and business contact information.

- (2) Identify and mark SBU data at document creation. You don't have to remove, mark, and restore unmarked SBU data already in records storage. If you remove unmarked SBU items from storage, you must mark them properly before processing or re-filing.
- (3) To mark sensitive data, TD P 15-71 requires that you:

Note: These marking requirements pre-date IRS implementation of the IRS Controlled Unclassified Information (CUI) program. Once implemented, CUI marking requirements will override SBU data marking requirements. For more information on CUI, refer to the *internal Controlled Unclassified Information site*.

Exception: Per IRM 1.11.2.5.3, Designate IRM Content as Official Use Only (OUO), the publishing process uses OUO for marking sensitive material and may continue this practice until the IRS implements the CUI program. Refer to IRM 11.3.12.3.1, Published Materials.

- a. Prominently mark items that include SBU data at the top or bottom of the front cover and each individual page with the marking “SENSITIVE BUT UNCLASSIFIED” or “SBU.” In the IRS, instead of **SBU**, you may use one of the markings in IRM 10.5.1.6.5 (4) to highlight its sensitivity and to clarify what type of SBU data.
 - b. Adjust information system prompts to include SBU data markings in headers and footers.
 - c. Mark portions, paragraphs, and subject titles that include SBU data with the abbreviation “SBU” to differentiate it from the remaining text. When the entire text has SBU data, the portion markings are optional.
 - d. Include a statement or marking alerting the recipient of the sensitivity, either in a transmittal letter or directly on the document, when sending SBU data outside the IRS, except when sending a taxpayer their own information. [TD P 15-71]
- (4) Not all markings must say “SBU.” Instead of using “SBU,” you may choose a more descriptive marking. Review the following table with markings based on the **source** of the data and the underlying law that protects it. For documents and sites in the M365™ environment (such as in email, Word™, Excel™, and PowerPoint™), consider using sensitivity labels that mirror these markings. FTI is the highest sensitivity, while Uncontrolled – not SBU is the lowest. Change your marking as needed, justifying the change if you lower the sensitivity. For more information, refer to the *internal Sensitivity Labels site*.

If the information is... [source]	Then mark as... [marking]
Tax information collected under our authorities to administer and enforce internal revenue laws, such as IRC 6103, or meets the definition of tax information in IRM 10.5.1.2.4, Federal Tax Information (FTI).	Federal tax information (FTI)
Non-tax information (not FTI) collected under IRC, but protected under the Privacy Act or otherwise meets the definition of PII in IRM 10.5.1.2.3, Personally Identifiable Information (PII).	Personally identifiable information (PII)
Not FTI or PII, but otherwise meets the definition of SBU data in IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data.	Sensitive but unclassified (SBU) data
Not sensitive and not FTI, PII, or SBU data	Uncontrolled – not SBU

- (5) Protective measures start when we apply markings and end when we cancel such markings or destroy records.
- (6) Although SBU is Treasury’s standard for identifying sensitive information, some kinds of SBU data might be more sensitive than others and call for more safeguarding measures beyond the minimum requirements shown here. Certain information might be extremely sensitive based on repercussions if the information is released or compromised – potential loss of life or compromise of a

law enforcement informant or operation. The IRS and its personnel must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel, property, or equipment for deciding the need for safeguards more than the minimum requirements here. Review IRM 10.5.1.2.11, High Security Items.

- (7) Place a *Sensitive But Unclassified (SBU) Cover Sheet, Other Gov TDF 15-05.11*, on documents with SBU data to prevent unauthorized or inadvertent disclosure when you remove SBU data from an authorized storage location and persons without a need-to-know are present or casual observation would reveal SBU data.
 - a. When sending SBU data, place an SBU cover sheet inside the envelope and on top of the transmittal letter, memorandum, or document.
 - b. When receiving SBU or equivalent information from another U.S. government agency, handle it following the guidance provided by the other U.S. government agency. Where no guidance exists, handle it following IRS policy as described here.

10.5.1.6.6
(09-15-2023)
Storage

- (1) For privacy-related concerns about electronic storage of SBU data (including PII and tax information):
 - For external sites, review IRM 10.5.1.6.9.7, Electronic and Online.
 - For internal collaborative electronic or online data sharing, review IRM 10.5.1.6.18, Data on Collaborative Technology and Systems, and IRM 10.5.1.6.18.3, Shared IRS Storage (OneDrive, SharePoint, Teams, and Other IRS Collaborative Sites).
- (2) For security-related concerns about electronic storage of SBU data (including PII and tax information), refer to IRM 10.8.1, Security Policy, about limiting access to need-to-know personnel and for encryption requirements.

Note: The IRS restricts the ability to save data on removable media storage devices. Refer to IRM 10.8.1.4.10, MP-01 Media Protection Policy and Procedures, and *internal removable media guidance (doc)*.

- (3) For physical security methods for protecting and storing physical SBU data (including PII and tax information) items, including high security and special security items, refer to IRM 10.2.14.3, Protecting Assets.
- (4) For storage of federal records, refer to the IRM 1.15 series, Records and Information Management.
- (5) For managers handling employee performance files (EPFs), refer to:
 - IRM 11.3.22.15, Maintaining Tax Return Information in Employee Performance Files.
 - IRM 6.430.2.3.5, Employee Performance File (EPF).
 - IRM 6.430.3.4.3, Employee Performance File (EPF).

10.5.1.6.7
(05-08-2025)
Phone

- (1) When talking about SBU data (including PII and tax information) via phone call, IRS personnel must:
 - a. Authenticate the individual. Review IRM 10.5.1.2.9, Authentication.
 - b. Confirm you're talking to an authorized person before discussing the information. Review IRM 10.5.1.2.10, Authorization.
 - c. Inform them you'll be talking about sensitive information.
 - d. Make sure no unauthorized people can overhear the conversation. Review IRM 10.5.1.6.7.1, Cell Phone or Cordless Device.

Note: While in an IRS office, you may still make phone calls, even though you might not be able to avoid other employees. However, you should minimize the potential for unauthorized disclosure (such as speak in a low voice or move to a conference room, if possible).

- (2) This subsection applies to talking on phone calls (including internet-based calls). For texting restrictions, review IRM 10.5.1.6.9.6, Text Messaging (Texting).
- (3) For security information on phones, refer to IRM 10.8.1.4.1.18.1, Telecommunication Devices.

10.5.1.6.7.1
(05-08-2025)
Cell Phone or Cordless Device

- (1) Remember that the use of cell phones or other cordless devices (cordless land lines) does not automatically create privacy and disclosure concerns, but use of these devices might raise some vulnerability issues. Refer to IRM 10.8.1.4.1.18.1, Telecommunication Devices, and IRM 10.8.1.4.1.19.1, Personally-Owned and Other Non-Government Furnished Equipment.
- (2) When possible, conduct cellular phone conversations in a private setting (and not in a crowded public setting) to minimize the potential for eavesdropping. Cordless devices are rarely, if ever, used outside of a person's home and do not lend themselves to conversations in crowded areas, but can still pose a risk of someone overhearing a conversation that the taxpayer does not want overheard.

Example: You may normally conduct a cell phone conversation from a private workspace within your home or from an automobile where you are the only occupant without someone overhearing the conversation. You may also conduct a conversation away from passers-by. Be careful not to convey sensitive information that others might overhear.

Caution: Be aware how loud you talk. Cell phone users tend to talk louder, often without realizing it.

- (3) For contacts initiated by IRS personnel that discuss SBU data (including PII or tax information), you must inform the other party you are calling from a cell phone or other cordless device when in a public place where others could overhear sensitive information. This will alert the other party of the potential for the inadvertent disclosure of their tax information. When calling from a private setting where others cannot overhear the conversation, you don't have to say the call is originating from a cell or cordless phone.

Example: When returning a call about sensitive information from a public place, say, "I'm calling you from my cell phone. Do you have the bank account information?" or, "I'm calling you from my cell phone. Do you have the

information about your tax return?" These or similar statements informing the person that you are calling from a cell phone are proper.

- (4) Even when you don't expect to discuss sensitive information in a call from a public place, you still should consider telling the other party you are using a cell phone or other cordless device in case a sensitive issue comes up in the discussion.

Example: "I'm returning your call from my cell phone. You wanted to set up an appointment?"

- (5) You must honor the other party's request not to conduct a conversation concerning sensitive information by cell or cordless phone. Offer them the choice of rescheduling the conversation when a private space or a more secure land line is available. Properly document any agreement (if documentation kept, such as history notes).
- (6) For taxpayer-initiated contacts, the IRS is under no obligation to find if the taxpayer is using a less secure platform such as a cordless device or cell phone. You can talk about SBU data (including PII or tax information) because the taxpayer accepted any security vulnerability by using such a device to contact the IRS.
- (7) Never discuss CNSI over a cell or cordless phone. For more about CNSI, refer to IRM 10.9.1.8, Safeguarding CNSI.
- (8) For information about text messaging or texting, review IRM 10.5.1.6.9.6, Text Messaging (Texting).

10.5.1.6.7.2
(05-08-2025)
**Answering Machine or
Voicemail**

- (1) Use the following for answering machine and voicemail guidelines when leaving messages with sensitive information:
- (2) You must not leave tax information protected by IRC 6103 on an answering machine or voicemail, but if you reasonably believe you have reached the taxpayer's or representative's correct answering machine or voicemail, leave your name, telephone number, any proper reference number for the inquiry, that you work for the IRS (identifying your function is permissible), and the name of the person who should return the call. You may leave more information on the recording if the taxpayer or representative has given prior approval to leave such information.
- (3) This supports reasonable belief:
 - The greeting on the answering machine or voicemail refers to the taxpayer or representative contacted, or
 - The taxpayer or representative has said this is the telephone number where you may reach them directly.
- (4) Document the taxpayer's or representative's telephone number, their approval to call that number, and their permission for the IRS to leave information on the recording.
- (5) Without reasonable belief that you have reached the correct taxpayer or representative, you must not leave any tax or other sensitive information on the message.

- (6) When you can't positively identify the number reached as the taxpayer's or representative's, ask for a return call without giving the taxpayer's name, if practical. If the call is in response to an earlier taxpayer inquiry or request, say the call is in response to an earlier inquiry or request. In such a case, you must not say the nature of the original situation nor reveal any specifics about the return call if it involves sensitive information.

Caution: When calling about collection of unpaid taxes, the restrictions of IRC 6304(b)(4) apply, and IRS personnel must not identify themselves as the IRS unless they reasonably believe the answering machine or voicemail belongs to the taxpayer or representative.

10.5.1.6.8
(05-08-2025)
**Email and Other
Electronic
Communications**

- (1) IRS personnel must use IRS email accounts or other IRS-approved secure electronic communication methods to conduct IRS official business. (TD P 85-01)
- (2) The Protecting Americans from Tax Hikes (PATH) Act of 2015, Section 402, Division Q of the Consolidated Appropriations Act of 2016 reads:

No officer or employee of the Internal Revenue Service may use a personal email account to conduct any official business of the government. [PATH]

Note: This policy applies to IRS officers, employees, and contractors alike, as noted in IRM 10.5.1.1.2, Audience. Law enforcement employees must refer to their divisional or law enforcement manuals for special rules.

- (3) Manage emails used for business communications as IRS records.
- (4) IRS personnel hold a legal responsibility to protect all IRS SBU data (including PII and tax information) entrusted to us by taxpayers, fellow personnel, and other individuals. This means communicating SBU data securely only with those authenticated, authorized individuals who have a need to know.
- (5) For external electronic communications, IRS personnel should use IRS-approved alternatives to email such as secure messaging or secure portals when available. Review IRM 10.5.1.6.8.6, Other Secure Electronic Communication Methods. Different policies apply for emails to taxpayers and representatives, other stakeholders, those with IRS accounts, and personal email. For more information about emailing outside the IRS, review the following subsections:
- IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives
 - IRM 10.5.1.6.8.2, Emails to Other External Stakeholders
 - IRM 10.5.1.6.8.3, Emails to IRS Accounts
 - IRM 10.5.1.6.8.4, Emails with Personal Accounts
- (6) When authorized to email SBU data, encrypt SBU data in emails using IRS IT-approved encryption technology. Do not include SBU data (including PII or tax information, such as the name control) in the email subject line. Review IRM 10.5.1.6.2, Encryption.

Caution: Encryption methods do not encrypt the subject line or the header (email address information).

Note: Review IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives, for subject line and header requirements.

(7) Examples of IRS IT-approved encryption technology include:

Internal (within the IRS network)	External (outside the IRS network)
Secure email encryption using the <i>Encrypt-Only</i> option. This encrypts the body of the email and attachments in transit.	<ul style="list-style-type: none"> • Recommended: Use alternatives to email. For alternatives to email, review IRM 10.5.1.6.8.6, Other Secure Electronic Communication Methods. For more information about when you can offer these alternatives, refer to your business unit procedures. • If alternatives are not available: Secure email encryption using the <i>Encrypt-Only</i> option. This encrypts the body of the email and attachments in transit. <p>Reminder: Encryption protects only the body of the email and attachments in transit, not the subject line. Do not put SBU data in the subject line.</p>

(8) Refer to the *internal Encryption site* for encryption instructions.

(9) Refer to these IRMs for more policy on email and other electronic communications:

- IRM 1.10.3.2, Security/Privacy.
- IRM 1.10.3.2.1, Secure Messaging and Encryption.
- IRM 1.15.6.9, Managing Electronic Mail Records.
- IRM 10.8.1.4.1.19 , AC-20 Use of External Systems.
- IRM 10.8.1.4.19.2.1, Electronic Mail (Email) Security.
- IRM 10.8.27-1, Prohibited Uses of Government Furnished IT Equipment and Resources.

10.5.1.6.8.1
(05-08-2025)

Emails to Taxpayers and Representatives

(1) Unless authorized by this policy in the limited allowable situations listed in this subsection, you must not send emails that include SBU data (including PII and tax information) to taxpayers or their authorized representatives, even if requested, because of the risk of improper disclosure or exposure.

Note: Special rules apply to personnel in previously approved secure email and messaging programs, such as LB&I and Chief Counsel employees. Refer to the *internal LB&I Secure Messaging Applications site* and the *Chief Counsel Directives Manual* for more information. For alternatives to email, review IRM 10.5.1.6.8.6, Other Secure Electronic Communication Methods.

Caution: Policies continue to apply in exigent circumstances. The IRS will post exceptions through *Interim Guidance* as needed.

- (2) When taxpayers request email contact and accept the risk of such, limited allowable situations without risking unauthorized disclosure of SBU data include:
 - a. Message sent under a previously authorized privacy- and IT-approved secure email or messaging program (rare). For example, the *internal LB&I Secure Messaging Applications site* or for alternatives to email, review IRM 10.5.1.6.8.6, Other Secure Electronic Communication Methods.

Note: Previously authorized programs are not the same as emails encrypted with IT-approved encryption.
 - b. Systemic message sent following IRM 10.5.1.6.8.5, Limited Exceptions to SBU Data Encryption.
 - c. Brief, unencrypted message confirming the date, time, or location of an upcoming appointment, but not the nature of the appointment. Do not include SBU data (including PII and tax information, such as the name control) in the email, subject line, or attachment. Do not allow follow-up email discussion of any taxpayer account or case.
 - d. Link to the publicly available forms and publications sections of IRS.gov. Avoid sending information about specific tax matters (revenue rulings, court cases, and specific IRS forms), which might unintentionally disclose the nature of a tax matter to an unauthorized third party.
- (3) Do not encourage or suggest taxpayers email SBU data (including PII and tax information) unencrypted or outside of a previously approved secure email program. For example, do not include an email address on correspondence that talks about SBU data.
- (4) When responding to unrequested emails from taxpayers or tax professionals, respond by letter or phone if possible; if address or phone number are not available, respond by email. You must:
 - a. Delete any SBU data (including PII and tax information) appearing in the original email or subject line. Some examples of phrases to watch for are “my situation” or “my information.”
 - b. Discourage the taxpayer from continuing the discussion by email.
- (5) A sample response to unrequested emails:

To protect your privacy, we discourage you from sending your personal information to us by unencrypted email. The IRS doesn't allow its personnel to exchange unencrypted sensitive information with email accounts outside of the IRS network, even with your permission. For further discussion about the matters in your original email, please contact us by telephone, fax, or mail.

10.5.1.6.8.2
(05-08-2025)
Emails to Other External Stakeholders

- (1) If you are authorized to email SBU data to authorized recipients, you may email SBU data (including PII and tax information) to those external stakeholders using IRS IT-approved encryption technology (review IRM 10.5.1.6.8, Email and Other Electronic Communications) only when the:
 - a. Individual is authorized to receive it under law or regulation, such as IRC 6103. Show authority by a formal request for information processed using established written procedures, or a memorandum of understanding or executed agreement which also uses email as the secure method of

transmission for the data. Review IRM 10.5.1.2.10, Authorization.

Note: The IRS Office of Safeguards does not authorize agencies subject to Pub 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, to email tax information (FTI). Refer to IRM 11.3.36.4, Implementing Requirements.

- b. Recipient needs the information for official duties.
- c. Recipient is authenticated.
- d. Recipient accepted information and any obligation to protect.
- e. Access controls limited to those with need to know.
- f. The applicable System of Records Notice (SORN) includes the use as a published routine use. Refer to the *internal System of Records site*.
- g. For tax information (FTI), sender follows policy in the IRM 11.3 series, Disclosure of Official Information.
- h. For non-tax PII, sender follows requirements in this IRM and IRM 10.5.6.2.2, Conditions of Disclosure Under the Privacy Act.

- (2) Do not encourage or suggest stakeholders email SBU data (including PII and tax information) unencrypted or outside of a previously approved secure email program.

Caution: Encryption methods do not encrypt the subject line or the header (email address information).

- (3) For when you receive emails with SBU data from external parties, review IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives.
- (4) Interact with applicants or prospective contractors by email only to answer questions about their information, qualifications, or administrative matters; minimize the exposure of their personal information (such as PII). Encrypt all emails with any personnel information.
- (5) For those who must provide the IRS with their SBU data (such as PII) for a business arrangement, ask them to fax, mail, or upload their SBU data to a secure system, such as USAJobs.

10.5.1.6.8.3
(05-08-2025)

Emails to IRS Accounts

- (1) IRS personnel must use IRS email for email communications with other IRS personnel about official business matters. They must encrypt all internal email messages with SBU data (including PII and tax information) using IT-approved encryption.

Caution: Encryption methods do not encrypt the subject line or the header (email address information).

- (2) For contractors, when provided with an IRS workstation as part of a contract, they must use their IRS workstation and account for all official communication (such as email or instant messaging). Refer to IRM 10.8.2.3.1.18, Contractor.

10.5.1.6.8.4
(05-08-2025)

Emails with Personal Accounts

- (1) No officer, employee, or contractor of the IRS may use a personal email account to conduct any official business of the government. [PATH] Three limited allowable circumstances include:

Note: Other options include using the official IRS email application in your IRS-issued device or Bring Your Own Device (BYOD) to add an attachment and send an encrypted email, or using an IRS scanner.

- (2) Personal Information – You may send your own SBU data (including your PII and your tax information) to or from your personal email accounts, if you encrypt it with IT-approved encryption. Examples may include your own:
- Personnel forms or records.
 - Financial records used to prepare an OGE Form 450 or OGE Form 278 or other form for financial reporting related to the job.
 - Records needed for a personal transaction.
 - Job application, resume, self-assessment, or appraisal.
 - Health records or fitness for duty information.
 - Travel itinerary (sent directly from ConcurGov by adding a personal email address for ConcurGov notifications related to their own travel, not approvals for others; personnel cannot send a travel itinerary from a work email address to a personal email address).

Exception: This encryption policy does not apply to your own PII that the IRS proactively makes available to all employees on resource sites (including Discovery Directory, Outlook™ (calendar, profile information [including profile photos], and address book), and SharePoint™ or Teams™ site collections [including profile photos]), such as names and business contact information.

- (3) Training or publicly available information – You may send non-case-related content, including links, to and from yourself when IT Security constraints prevent access. Examples of this include online training or meetings, such as webinars and seminars, as well as publicly available information (including public profile photos or business photos intended for publication with permission of pictured individuals).

Note: If you can access IRS training from IRS equipment, use the IRS equipment. You must not send IRS training material to your personal email.

- (4) Exigent circumstances, such as in emergencies. This includes when the IRS network is down and there is an urgent need to communicate or in disaster recovery situations, and you do not have other options. Limit SBU data to that necessary for the situation. Encrypt necessary SBU data with IT-approved encryption. Examples may include:
- Sending infectious disease-related documentation to an IRS email account when you do not have other options.
 - Reporting for work.
 - Assessing the condition or availability of the workplace.
 - Dealing with an emergency (internal to IRS, not taxpayer communication).
 - Checking the well-being of IRS personnel.
- (5) If you use personal email in exigent circumstances, you must copy (or send to or from) an IRS email account at the same time to make sure you keep a record of the communication in the IRS email system for transparency and information management purposes.

10.5.1.6.8.5
(05-08-2025)
**Limited Exceptions to
Email SBU Data
Encryption**

- (1) The general rule for encrypting SBU data (including PII and tax information) in emails shows the IRS's priority to protect sensitive information from unauthorized disclosure causing a risk of loss or harm to individual privacy or to IRS data.
- (2) After evaluating business needs with potential risk, refer to the following limited exceptions for encryption in external emails.

Caution: Do not include SBU data (including PII or tax information), such as the name control, in the email subject line. Encryption methods do not encrypt the subject line or the header (email address information).

Limited exception	Requirements
Subject line of case-related emails to the Department of Justice	<ol style="list-style-type: none">a. When IRS personnel communicate with the Department of Justice about existing docketed court cases, personnel may include the docketed case name and docketed filing number in the subject line of those emails. If the full name is not part of the case name, then do not use the full name.b. This information fits within the judicially created public records exception to IRC 6103, recognized in most jurisdictions. Refer to IRM 11.3.11.12, Information Which Has Become Public Record, for more information on the public records exception.c. If the body of an email or any attachment has other SBU data, IRS personnel must encrypt both the email and attachment using IT-approved technology.
Emails generated to taxpayers or representatives by approved online applications	<ol style="list-style-type: none">a. The IRS online applications may issue emails to taxpayers or representatives, without encryption, when the messages have no SBU data and only incidental information (not tax information, which includes payment amount, address change, or type of notice) to:<ul style="list-style-type: none">• Confirm authentication.• Inform a user that a secure message is available for viewing in an IRS online application (without details).• Confirm an online transaction (without details).b. This exception is limited to the following circumstances:<ul style="list-style-type: none">• The email is automatically generated by an approved IRS application, and• The taxpayer or representatives consented to these notices by completing the application's enrollment process. During this enrollment process, the taxpayer or representative must have received clear notice of the IRS's intent to send such notices via email.c. Privacy Policy must review and approve online application email content. For approval or questions, email <i>*Privacy</i>.
IRS employees sending their personal SBU data via IT-approved encrypted email. Personal SBU data is information only about you.	<ol style="list-style-type: none">a. You may choose to send your personal SBU data outside the IRS via encrypted email or a password-protected encrypted attachment.b. This exception does not include IRS usernames and passwords.c. For privacy policy on encryption, review IRM 10.5.1.6.2, Encryption.d. Refer to the <i>internal Encryption site</i> for encryption instructions.

Limited exception	Requirements
Emergency emails by Facilities Management and Security Services (FMSS)	<ol style="list-style-type: none"> a. Where significant incidents (as defined in IRM 10.2.8.2, Incident Report) occur, and FMSS employees need to supply law enforcement entities with detailed information, but cannot do it expediently by phone, they may use unencrypted email to send the necessary details, including SBU data. b. FMSS employees must make every effort to minimize the amount of SBU data within those messages (for example, no SSNs).

10.5.1.6.8.6
(05-08-2025)

Other Secure Electronic Communication Methods

- (1) The IRS offers some alternatives to email to protect taxpayer security and privacy:
 - a. Secure Messaging platform (formerly Taxpayer Digital Communication (TDC)): Taxpayers must register, but can then send and receive messages on an encrypted platform. For the internal login page, refer to the *internal Secure Messaging site*.
 - b. Document Upload Tool (DUT): The IRS initiates access to the tool by providing the link and, in some cases, unique access code or ID, through a notice, phone conversation or in-person visit. This is a one-way (public to IRS) encrypted communication. Refer to the *IRS Document Upload Tool (external) site*.
 - c. Secure Large File Transfer (SLFT): Hosted by Kiteworks, use this for large file transfer, with proper authentication and authorization. For more information, refer to the *internal Secure Large File Transfer (SLFT) site*.
- (2) These examples of IRS-approved alternatives might not be your only options. Check with your business unit for other secure communication methods.

10.5.1.6.9
(12-31-2020)

Other Forms of Transmission

- (1) This subsection addresses forms of transmission other than phone and email.
- (2) You must provide adequate safeguards for SBU data (including PII and tax information) sent from one location to another.

10.5.1.6.9.1
(05-08-2025)

Field and Travel

- (1) When IRS personnel carry SBU data (including PII and tax information) in connection with a trip or during daily activities, they must protect it and keep it with them when possible.

Note: Protecting SBU data includes avoiding encounters with smart devices that can record. Review IRM 10.5.1.6.20, Smart Devices.

- (2) If you must leave SBU data (including PII and tax information) unattended in an automobile while traveling between work locations or between work and home, lock it in the trunk of the locked vehicle. If the vehicle does *not* have a trunk, conceal the material from plain view and secure it in some manner in the locked vehicle. When not in transit, secure data in an approved work location (office, approved and securable telework location, or approved taxpayer site in IRS-approved lockable containers). In either case, leave the material unattended for only a **brief period**.
- (3) If you must leave the SBU data (including PII and tax information) unattended in a hotel or motel room, lock it in a briefcase and conceal it when possible.

- (4) When moving SBU data (including PII and tax information) from one building to another (even within the same campus) or one location to another even if a short distance, take necessary steps to protect the information from unauthorized disclosure, loss, damage, or destruction.
- (5) Field employees might have SBU data needing protection while temporarily stored at the taxpayer's site.
 - a. Store SBU data (such as agent's work papers, original returns, examination plans, probes, or fraud data) housed unattended at the taxpayer's site in a container under the control of the responsible IRS employee. If possible, use an IRS-furnished security container. If necessary, use a taxpayer-furnished container, but change the taxpayer-furnished container (such as with bars and locks) so the taxpayer cannot access the container.
 - b. During duty-hours, the SBU data must be under the personal custody of the IRS employee if not properly secured in approved containers.
 - c. If you don't have a lockable and suitable container provided, you must not leave SBU data at the taxpayer's site.
- (6) For more information about how to protect a taxpayer's location when using GPS and location services, review IRM 10.5.1.6.11, Global Positioning Systems (GPS) and Location Services.

10.5.1.6.9.2
(05-08-2025)
**Mail through United
States Postal Service
(USPS)**

- (1) Use United States Postal Service (USPS) for all mail sent to taxpayers and their representatives. Refer to IRM 1.22.5.10, Acceptable Mail/Shipping Services.
- (2) IRS personnel must follow proper data protection procedures when mailing SBU data (including PII and tax information). For more information on IRS policy about mail operations, refer to IRM 1.22.5, Mail Operations.
- (3) For telework mail procedures, refer to IRM 6.800.2.3.4.7, Mail, and IRM 1.22.5.11, Guidance on Telework Employee Mail.
- (4) When sending SBU data by mail **within the U.S. and Territories** (served by USPS):
 - a. Place SBU data in a single opaque envelope or container.
 - b. Seal it to prevent inadvertent opening and to reveal evidence of tampering.
 - c. Clearly show the complete name and address of the sender and intended recipient or program office on the envelope or container.

Note: Mailroom personnel may open and examine SBU data the same way they evaluate and verify other incoming mail safe for internal delivery. You must mail SBU data by USPS First Class Mail. You may use express mail services or commercial overnight delivery service, as necessary.

- (5) When sending SBU data to offices **Overseas**:
 - a. If serviced by a military postal facility (such as APO, FPO, or DPO), mail SBU data directly to the recipient using USPS (regardless of letter or package weight). You must use USPS when mailing to a post office box, APO, FPO, or DPO.

- b. Where a military postal facility does not service the overseas office, send the information through the Department of State's (DOS's) unclassified diplomatic pouch. Coordinate in advance with DOS officials to make sure delivery at the final destination meets IRS needs and DOS schedule for such deliveries.

10.5.1.6.9.3
(05-08-2025)

Shipping through Private Delivery Carrier

- (1) You must ship packages with SBU data (including PII and tax information) that weigh 13 ounces or more through a private delivery carrier.

Exception: Even if more than 13 ounces, use USPS for all mail sent to taxpayers and their representatives. Refer to IRM 1.22.5.10, Acceptable Mail/ Shipping Services.

- (2) IRS personnel must follow proper data protection procedures when shipping SBU data through a private delivery carrier. This practice helps prevent data loss and disclosure, and in case of loss or disclosure, allows the IRS to notify affected individuals.
- (3) For Telework shipping procedures, refer to IRM 6.800.2.3.4.7, Mail, and IRM 1.22.5.11, Guidance on Telework Employee Mail.
- (4) For shipping electronic media, including removable media such as USB drives and other portable storage devices, you must encrypt it first. Refer to IRM 10.8.1.4.10.4, MP-05 Media Transport.

Note: The IRS restricts the ability to save data on removable media storage devices. Refer to IRM 10.8.1.4.10.6, MP-07 Media Use (InTC), and *internal removable media guidance (doc)*.

- (5) For all SBU data shipments through a private delivery carrier, the sender must follow the procedures included below for properly double packaging, double labeling, and tracking the shipment, including the use of Form 3210, Document Transmittal (or equivalent). Whether you use a Form 3210 or its equivalent, you must include enough information on the transmittal to identify the package contents in case of its loss or disclosure, so the IRS can notify affected individuals and take steps to decrease the possibility that the information will be compromised or used to perpetrate identity theft or other forms of harm.

Note: The equivalent transmittal might be a cover letter listing enclosures, of which the IRS keeps a copy.

Exception: You must continue to send mail to post office boxes via USPS (regardless of letter or package weight). You must use USPS when mailing to a post office box, APO, FPO, or DPO.

- (6) When shipping SBU data through private delivery carrier, you must use UPS CampusShip at all non-Campus locations and non-FMSS-contract-mailroom-supported offices; Campus locations and FMSS-contract-mailroom-supported offices may use UPS CampusShip, but it is not mandatory at those locations. UPS CampusShip is an internet-based shipping system that you can access from any location that has internet access. The IRS has rolled out UPS CampusShip across the country to IRS field offices not serviced by a FMSS contract mailroom. Find information about UPS CampusShip:

- *Shipping Packages (Mailrooms and UPS CampusShip) site.*
- Document 12888, UPS CampusShip: Electronic Shipping Methods.
- Document 12889, UPS CampusShip: Advanced Features.

(7) CampusShip allows employees to:

- a. Generate labels electronically.
- b. Secure current IRS address information from a corporate address repository to improve accuracy of delivery.
- c. Track packages via the internet to easily verify their shipments arrived at the intended destination and to quickly find a missing shipment, reducing the likelihood of SBU data loss or disclosure to an unauthorized individual.
- d. Let recipients know a package is coming by adding their email address to CampusShip for notifications.

(8) You must double-package and double-label SBU data packages before shipping. Double-packaging helps protect the contents if the outer package is damaged or destroyed during the shipping process. Duplicate shipping labels allow proper delivery of the contents without potential disclosure if the external package is damaged or destroyed.

Caution: Shrink wrapping the external packaging or wrapping the external packaging in paper does not satisfy double packaging requirements.

(9) Evaluate the size of the SBU data shipment and identify proper packing materials. The proper kind of internal and external packaging depends upon the size and weight of the package. Use the smallest size packaging to reduce shipping costs and ensure minimal shifting of contents during shipment.

(10) The sender must also decide whether to ship via ground service or express (Overnight and Second Day Air) services:

- Use **Ground service** for shipping when possible. Ground service should always be the first choice; use express services only when necessary. There is no requirement to mail SBU data via express services. For distances up to 500 miles, the regular ground service offered by the small package or motor freight carriers (depending on weight of shipment) can deliver your shipment within one or two days. For ground shipments, the business operating divisions supply the packaging material.
- **Express Services** are the fastest mode of transportation available, but they are also much more expensive. Only use this mode when transit time requirements are short and the urgency of the shipment outweighs the added costs involved (for example, remittances, statute cases, or tax court cases) Only use small package carrier-provided packaging (carrier branded envelopes and boxes) for express services and when provided at no cost.

(11) For all SBU data shipments through a private delivery carrier, the sender must prepare Form 3210, Document Transmittal (or its equivalent), identifying the package contents for all packages with SBU data and asking for recipient acknowledgement. This practice includes shipments to IRS offices, contractors, and external agency partners, when applicable. For external partners, use an equivalent to Form 3210. Whether you use a Form 3210 or its equivalent, you must include enough information on the transmittal to identify the package

contents in case of its loss or disclosure, so the IRS can notify affected individuals and take steps to decrease the possibility that the information will be compromised or used to perpetrate identity theft or other forms of harm.

- a. For easier tracking, the sender may include the small package carrier tracking number in the **Remarks** area in Part 4 (sender's copy) of Form 3210 (or equivalent).
- b. If the sender is using the small package carrier's web-based system to electronically generate shipping labels, the tracking number is available immediately on the shipping label.
- c. If the sender is using a contract mailroom, the sender should complete the sender's email address section of Form 9814, Request for Mail/Shipping Service. The mailroom must enter this email address when preparing the shipping label, and the small package carrier software will generate an email to the sender with the tracking number. The sender can then place the tracking number on Part 4 of Form 3210 (or equivalent) for proper record keeping.
- d. If using a transmittal form other than 3210 as its equivalent, include at least the same elements you would on a Form 3210.

Caution: Redact SSNs on Form 3210 (or equivalent) to show only the last four digits. Do not include the full SSN on Form 3210 (or equivalent). To help identify affected individuals in case of loss or disclosure, also include the name control and at least one other element (such as zip code) to allow for account lookup. When you use an official letter as a Form 3210 equivalent, the SSN may not be present. Make sure that enough information is available on the letter to identify affected individuals in case of loss or disclosure.

- (12) Securely package the SBU data by placing the contents and the properly completed Form 3210 (or equivalent) in a properly sized internal package. The sender keeps Part 4, Sender's copy, of Form 3210 (or equivalent) and includes Part 1, Recipient's copy, and Part 3, Acknowledgement copy, with the shipment. When you use a transmittal letter as an equivalent of Form 3210, the shipment does not require a paper equivalent to Form 3210 Part 3; the recipient's verbal or electronic confirmation of receipt suffices as acknowledgement. When sending the package to a specific individual, the sender may choose to notify the recipient via encrypted email, phone, or other method that the package with SBU data is on its way before shipping it. The sender may also choose to send an electronic PDF version of Form 3210 (or equivalent) via encrypted email to the intended recipient, so the recipient is aware of the expected shipment.

- (13) Internal packaging may include any of the following:

- **An envelope:** An E-20, Confidential Information envelope, is acceptable for this purpose.
- **An approved inner security shipping bag:** Should be sturdy enough to support the weight of the contents without tearing; should be opaque so the contents are not readable through the bag. For more information, refer to the *internal How to Order Inner Packaging Supplies (pdf)*.

Note: We recommend this as the easiest and most cost-effective method for double packaging large case file shipments.

- **A small box:** An undamaged smaller box that fits within the external shipping box.

Order internal packaging for ground shipping through the Order and Subscription Management System (OSMS). For more information on kinds of internal packaging available, refer to the *Ground Shipping Supplies* site.

- (14) Label the internal package with the following information:
- a. Send to Address, including Mail Stop or Drop Point Number, if applicable.
 - b. Return Address, including Mail Stop or Drop Point Number, if applicable.
 - c. Sender's phone number.
 - d. Small Carrier tracking number, if available.
- (15) The sender may use a copy of the CampusShip electronically generated exterior shipping label for the internal label, so print 2 copies (the first for the interior, the other for the exterior).
- (16) Place the properly labeled, packaged, and sealed internal package into the external package. External packaging materials may include:
- a. **Envelope:** For shipping smaller case files and documents via ground service, use an IRS issued non-confidential envelope (E-44; minimum size 9 ½" X 12"). Use an envelope or padded pack provided by the Small Package Carrier only when time constraints require shipping via express services.
 - b. **Box:** Use an undamaged box specifically designed for shipping. Choose a box strength that is suitable for the size and weight of the contents you are shipping. For shipping smaller packages up to 10 pounds, use a small box ordered from an office supply vendor for ground shipments. Use boxes provided free of charge by the small package carrier only when time constraints require shipping via express services. For shipments over 10 pounds, the external box should be a suitable flap top, corrugated cardboard box rated with a bursting strength to support the contents. Never exceed the largest gross weight for the box, usually printed on the box maker's certificate on the bottom flap of the box.
- Note:** A standard shipping record box (size 14.75" X 12" X 9.5") used to retire files meets this requirement. If possible, use the shipping record box sleeve as the external packaging. File boxes used for Federal Record Center storage, with a sleeve box, will have a bursting strength exceeding 125 pounds per square inch and will be more than adequate for most ground shipments.
- Caution:** Used copy paper boxes and other boxes with lids do not meet this requirement; boxes with lids can catch on conveyer belts and damage or destroy the shipment.
- (17) When possible, use a new box, but you may re-use undamaged packaging materials to ship SBU data. Only reuse a box if it is rigid and in good condition with no punctures, tears, rips, or corner damages, and all flaps are intact. Remove any existing labels and all other shipment markings if re-using a box.
- (18) Use enough packing material inside the package so the contents do not move or shift when shaken.

- a. Cushioning material should consist of materials that are readily available, and you can re-use them. It is not necessary to buy prefabricated materials specifically designed to cushion packages for this purpose.
 - b. Examples of cushioning material include non-confidential paper, shredded administrative paper, obsolete forms, newspaper, and commercially bought styrofoam peanuts, air bags, and such.
 - c. Place the cushioning material around the items in the box. Close and shake the box to check whether you have enough cushioning material; add more cushioning material if you hear or feel the contents shifting.
- (19) Do not mark or label external packaging material with information showing that package contents include sensitive information. You can mark packages as “time sensitive” or “process immediately” as applicable to ensure prompt processing. Labels that show sensitive contents include:
- “Remittance” labels saying package contents include remittances.
 - Labels showing package contents include case files or re-files. An acceptable alternative method would be to write “Sort and Sequence.”

Note: Do not remove references to the IRS from an envelope since it is necessary to include the IRS on the return address and send to address labels to ensure package delivery to the intended location if any of the address information is incorrect.

- (20) Seal the package with strong clear shipping tape that is two inches or more in width. Do not use string, paper over-wrap, shrink wrap, or plastic straps.
- (21) Place the shipping label on the top of the package and make sure it is properly attached and will not separate from the box. Do not place the label over a seam or closure or on top of sealing tape since this could cause it to be damaged or removed from the package.
- (22) The sender must monitor the shipment delivery. Follow your organization’s time frames for Form 3210 (or equivalent) acknowledgement follow-up. Where there is no time frame in an individual organization, the follow-up action should take place in three business days for overnight shipments and 10 business days for ground shipments.
- (23) Once received, the recipient will verify receipt of the contents and sign the acknowledgment copy of the Form 3210 (or equivalent). The recipient will return the Form 3210 (or equivalent) acknowledgement to the sender using secure email (electronic or scanned copy), fax, or mail. If the SSN was not redacted as required on the Form 3210 (or equivalent), redact all but the last four digits of the SSN before returning it to the sender.

Exception: When you use a transmittal letter as an equivalent of Form 3210, the shipment does not require a paper equivalent to Form 3210 Part 3; the recipient’s verbal or electronic confirmation of receipt suffices as acknowledgement.

- (24) After receiving the acknowledgement copy (if applicable, equivalent confirmation of receipt), the sender will associate it with the original Form 3210 (or equivalent). No further action is required after the sender receives the signed Form 3210 (or equivalent) acknowledgement and associates it with the original Form 3210 (or equivalent).

- (25) If you do not receive the signed Form 3210 acknowledgement (or equivalent confirmation of receipt) within the time frame, access the small package carrier's website to track whether the shipment arrived successfully. The tracking number should have been on Form 3210 (or equivalent) before shipment.
- (26) If the tracking information shows the package **arrived**, the sender must contact the intended recipient to confirm actual receipt of the package.
 - a. If the recipient did receive the package, ask the recipient to complete and return the Form 3210 (or equivalent) acknowledgement. If applicable, document alternative verbal or electronic confirmation of receipt.
 - b. If the recipient didn't receive the package, consider the package lost. The sender must follow the procedures for reporting a loss of hardcopy documents. The intended recipient should also start a search in their facility when the carrier shows an individual signed for the package.
- (27) If the tracking information shows the package **did not arrive**, the sender should closely monitor the tracking information for up to 48 hours (2 business days) after the expected delivery date for air services and up to 72 hours (3 business days) after the expected delivery date for ground services. If not delivered within these time frames, consider the package lost. The sender must follow the procedures for reporting a loss of hardcopy documents.
- (28) Immediately upon discovering or identifying a package is lost, report the loss following IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures. Refer to the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.
- (29) Business unit management must set up an internal process to identify the package contents and affected individuals in case of a lost or compromised package. We must be able to identify the contents of the lost package and help the carrier verify whether it belongs to the IRS. You must provide detailed information about the contents such as taxpayer last names, check numbers, forms numbers, and documents enclosed, including all identifying information that might help locate the contents of the package.
- (30) Managers must perform, at a minimum, quarterly audits of the Form 3210 (or equivalent) acknowledgement process for packages with SBU data to make sure proper follow-up is occurring. Managers must document the results of these audits. This procedure will allow IRS managers the opportunity to confirm that SBU data senders are following up on Form 3210 (or equivalent) acknowledgments within defined time frames so that they identify lost shipments quickly. This reduces the likelihood of exposing SBU data to an unauthorized user. Local management must decide the proper follow-up time frame as part of the manager's operational review. Keep Form 3210 (or equivalent) following the existing record retention schedule for each business unit.
- (31) Management should periodically sample mail to make sure the business unit follows this SBU data shipping policy.
- (32) For more information, refer to the *internal Shipping Policy and Procedures for Packages Containing SBU and Sensitive PII Documents site*.
- (33) Refer to IRM 1.15.5.9, Shipping Permanent Records to NARA, for shipping records (such as tax or personnel records) to the Federal Records Centers.

10.5.1.6.9.4
(05-08-2025)
Faxing

- (1) Protect faxed SBU data (including PII and tax information) as with any other transmission of SBU data.
- (2) For detailed procedures on how to safely fax sensitive information, including to taxpayers and their authorized representatives, refer to IRM 21.1.3.9, Mailing and Faxing Tax Account Information. Also refer to the *internal Faxing site*.
- (3) Internally, use secure encrypted email, if possible, as an alternate way to send SBU data, instead of faxing. Scan, encrypt, and internally email documents that include SBU data. Review IRM 10.5.1.6.8, Email and Other Electronic Communications.
- (4) If you must fax the information, do not send SBU data to a fax machine without contacting the recipient to arrange for its receipt.
- (5) Use a cover sheet for faxes with SBU data that lets the recipient know that it has sensitive information and requests unintended recipients to report the disclosure and confirm destruction.
- (6) For misdirected faxes, refer to IRM 10.5.4.3.5, **No Reporting** Situations.
- (7) When sending SBU data via fax, use Enterprise e-Fax (EEFax) as the preferred method of faxing documents. Refer to the *internal EEFax site*.
- (8) For more information on securely faxing documents, refer to IRM 10.8.1.4.18.7, SC-08 Transmission Confidentiality and Integrity.

10.5.1.6.9.5
(05-08-2025)
Printing

- (1) Protect printed documents with SBU data and follow the IRS clean desk policy in all work locations (including field and telework). Review IRM 10.5.1.5.1, Clean Desk Policy.

Note: Remember to retrieve printed items from the printer as part of following the clean desk policy.

- (2) Minimize the printing of SBU data to what is explicitly necessary.
- (3) Properly store and dispose of printed materials. Review IRM 10.5.1.6.6, Storage, and IRM 10.5.1.6.10, Disposition and Destruction.
- (4) Use only IRS-furnished (not personally owned) printers. Refer to IRM 10.8.1.4.1.19.1, Personally-Owned and Other Non-Government Furnished Equipment.

10.5.1.6.9.6
(05-08-2025)
Text Messaging (Texting)

- (1) The IRS may use limited automated, system-generated (or system user-initiated), one-way text messaging to send generic, non-sensitive information with prior consent. The messages must not include SBU data (such as personnel information or taxpayer case data).
- (2) Do not include SBU data in texts because any transmission of SBU data must meet encryption requirements in IRM 10.8.1.4.18.7, SC-08 Transmission Confidentiality and Integrity.
- (3) Automated, system-generated short one-way event or time-based text messages sent on behalf of the IRS must follow the policy for emails generated to taxpayers or representatives by approved online applications in IRM 10.5.1.6.8.5, Limited Exceptions to Email SBU Data Encryption.

- (4) Any other text messaging (texting) for official business remains prohibited.
- (5) Privacy policy must review and approve system-generated message content. For questions and approval, email **Privacy*.
- (6) Refer to IRM 1.15.6.16.1, Agency-approved Electronic Messaging (and any related interim guidance).
- (7) Refer to IRM 10.8.1.4.1.18.1, Telecommunication Devices.

10.5.1.6.9.7
(05-08-2025)
Electronic and Online

- (1) External electronic transmission and online data exchanges address uploading or downloading, secure file transfer, file sharing, peer-to-peer (P2P), collaborative technology and systems, third-party sites (commercially available file-sharing sites in the cloud or private file-sharing on remote servers), and blocked or blacklisted sites.

Note: For more information about when this is acceptable, refer to IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data.

- (2) Do not post or upload SBU data (including PII and tax information) online, including IRS official internal or external websites or cloud-based systems or services, unless secured with IT-approved access controls by the IRS (or by an IRS vendor bound by contract to protect the information). [NIST SP 800-122, TD P 85-01]

Note: This policy does not apply to SBU data the IRS proactively makes available to all IRS personnel on internal resource sites (including Discovery Directory, Outlook™ (calendar, profile information, and address book), and SharePoint™ or Teams™ site collections), such as names, SEID, and business contact information.

- (3) Use only IRS identifiers (name or email) when conducting official business.

Note: Never use personal email accounts for IRS business. [PATH]

- (4) Review IRM 10.5.1.6.8.6, Other Secure Electronic Communication Methods. For internal collaborative electronic or online data sharing, review IRM 10.5.1.6.18, Data on Collaborative Technology and Systems, and IRM 10.5.1.6.18.3, Shared IRS Storage (OneDrive, SharePoint, Teams, and Other IRS Collaborative Sites).
- (5) For more information about securing electronic transmissions, refer to IRM 10.8.1.4.1.19, AC-20 Use of External Systems, and IRM 10.8.1.4.17.8, SA-09 External System Services.
- (6) For more information about secure emailing, review IRM 10.5.1.6.8, Email and Other Electronic Communications.

10.5.1.6.9.8
(12-31-2020)
**Information Privacy
During Office Moves**

- (1) When moving an office or material, make plans to protect and account for all SBU data (including PII and tax information), as well as government property. Consider the relevant factors of the move (such as the distance involved and the method used in making the move).
 - a. Keep SBU data in locked cabinets or sealed packing cartons while in transit.

- b. Make sure that cabinets or cartons do not become misplaced or lost during the move.
- (2) Take precautions equal with the type and value of property and data involved.

10.5.1.6.10
(05-08-2025)
**Disposition and
Destruction**

- (1) Destroy documents with SBU data (including PII and tax information), also known as sensitive waste material, by properly shredding, burning, mulching, pulping, or pulverizing beyond recognition and reconstruction. If other sources for these requirements conflict, use the most stringent requirements. [TD P 15-71, Treasury Security Manual, Chapter III, Section 16, Destruction of Classified and Sensitive Information, and Section 24, Sensitive But Unclassified Information]

Note: While PGLD owns this policy, FMSS owns the Sensitive Document Destruction (SDD) program. Refer to the *internal FMSS SDD program site*.

- (2) Follow specific instructions for different kinds of materials and situations:
- a. IRM 10.5.1.6.10.1, Hardcopy Paper Disposition and Destruction
 - b. IRM 10.5.1.6.10.2, Electronic Disposition and Destruction
 - c. IRM 10.5.1.6.10.3, Microforms Disposition and Destruction
 - d. IRM 10.5.1.6.10.4, Temporary Storage Disposition and Destruction
 - e. IRM 10.5.1.6.10.5, Records Management Disposition and Destruction
 - f. IRM 10.5.1.6.10.6, Contractors Disposition and Destruction
 - g. IRM 10.5.1.6.10.7, Recycling Disposition and Destruction
- (3) Sensitive waste material may include extra copies, photo impressions, microfilm, printouts, computer tape printouts, IDRS printouts, notes, work papers, CDs, USB drives or other removable media, or any other material with SBU data (including PII and tax information) which has served its purpose.
- (4) Bring all sensitive waste material for destruction into the office for proper disposition, even when teleworking with access to a shredder at home. It's not necessary to transport sensitive waste in a locked receptacle, but you must still be careful to protect it during transit.

Note: In exigent circumstances, or if under evacuation orders, work with your manager to safely arrange this.

- (5) Do *not* discard sensitive waste material, including that shredded with non-compliant equipment, in regular trash bins.
- (6) Protect sensitive waste as you do any other SBU data (including PII and tax information). Material identified for destruction does not change the requirement to provide proper protective measures. Protect sensitive waste material as required for the most protected item.
- (7) Keep waste material in a secured (locked) container in a secured area to prevent SBU data from unauthorized disclosure or access.

Note: The only exception to this policy is for pipeline activities subject to a clean desk policy waiver. Review IRM 10.5.1.5.1, Clean Desk Policy.

- (8) Although IRS personnel might know the proper methods of destroying tax data, management must reinforce this knowledge by including document destruction as a topic in orientation sessions, periodic group meetings, and other awareness sessions.
- (9) Managers must periodically review work areas to make sure employees discard sensitive waste material properly.

10.5.1.6.10.1
(05-08-2025)
**Hardcopy Paper
Disposition and
Destruction**

- (1) Place hardcopy waste material with SBU data in locked receptacles specifically marked for sensitive document destruction (SDD or shred bins). This includes material shredded with non-compliant equipment that does not meet requirements.

Exception: Burn bags or shred boxes for Temporary Storage. [TD P 15-71, Treasury Security Manual, Chapter III, Section 16, Destruction of Classified and Sensitive Information]

- (2) For one-step destruction of paper with SBU data, use cross-cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize or disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. [NIST SP 800-88, Guidelines for Media Sanitization]
- (3) When shredding, you must procure and use the same equipment approved for destroying Secret or Confidential classified information (CNSI). Refer to the current *National Security Administration/Central Security Service (NSA/CSS) Evaluated Products List (EPL) (external)* for compliant shredders. [TD P 15-71, Treasury Security Manual, Chapter III, Section 16, Destruction of Classified and Sensitive Information]
- (4) For multi-step destruction of paper, you may use non-compliant methods for the first step. The IRS must then protect the product until destroyed in a way that makes it unreadable, indecipherable, and irrecoverable. [32 CFR 2002]

10.5.1.6.10.2
(05-08-2025)
**Electronic Disposition
and Destruction**

- (1) For electronic media destruction requirements (for items such as magnetic media, diskettes, hard disks, CDs, external drives, USB drives or other removable media, or other storage devices), refer to IRM 10.8.1.4.10.5, MP-06 Media Sanitization, and follow NIST SP 800-88, Guidelines for Media Sanitization.
- (2) Refer to the *internal Media Destruction Shipping Procedures (pdf)* for disposal of electronic media.
- (3) Do not put electronic media with hardcopy paper in the sensitive document destruction bins.

10.5.1.6.10.3
(07-08-2021)
**Microforms Disposition
and Destruction**

- (1) For microforms with SBU data (microfilm, microfiche, or other reduced image photo negatives): [NIST SP 800-88, Guidelines for Media Sanitization]
 - a. Destroy microforms by burning.
 - b. Do not put microforms with hardcopy paper in the sensitive document destruction bins.

10.5.1.6.10.4
(05-08-2025)
**Temporary Storage
Disposition and
Destruction**

- (1) For temporary storage, while waiting for destruction of sensitive waste, you don't have to put it in a locked receptacle if you follow these requirements for burn bags or shred boxes:
 - a. Tear and place SBU data to be destroyed in **sealed opaque** containers, commonly known as burn bags or shred boxes, so that the sensitive information is not visible.
 - b. Protect burn bags or shred boxes awaiting destruction while in your custody.
 - c. Make sure only authorized personnel collect burn bags or shred boxes and destroy their contents.
 - d. If not in your custody, store burn bags or shred boxes within a sensitive compartmented information facility (SCIF) or security-approved open storage area pending collection by authorized personnel.
 - e. Never leave unattended any burn bags or shred boxes outside a SCIF or open-storage area.

[TD P 15-71, Treasury Security Manual, Chapter III, Section 16, Destruction of Classified and Sensitive Information]

10.5.1.6.10.5
(05-08-2025)
**Records Management
Disposition and
Destruction**

- (1) Manage IRS records (hardcopy and electronic), including those with SBU data (such as PII and tax information), properly and follow the Records Control Schedules (RCS) Document 12990 and General Records Schedules (GRS) Document 12829 to prevent unlawful or unauthorized destruction of records.
- (2) You must have an approved Form 11671, Certificate of Records Disposal for Paper or Electronic Records, before destruction of any original federal records. Refer to IRM 1.15.3.8, Form 11671, Certificate of (In-house) Records Disposal.
- (3) Disposition and destruction of tax information must follow the IRM 1.15 series, Records and Information Management.

10.5.1.6.10.6
(05-08-2025)
**Contractors Disposition
and Destruction**

- (1) Turn over unshredded sensitive information to a contractor provided the contract includes necessary safeguards that follow IRC 6103(n) requirements, provides for periodic safeguard reviews, and includes language describing methods of collection, pick-up, storage, and disposition. Refer to IRM 11.3.24.3.7, Destruction of Returns and Return Information.
- (2) If an independent contractor collects and destroys tax information media, to prevent the necessity of having an IRS employee present during destruction, the contract must include the safeguard provisions required by IRC 6103(n) and regulations.
 - a. The provisions of the contract must allow for IRS inspection of the contractor facility and operations to ensure the safeguarding of IRS information.
 - b. Contractors must keep waste material in a secured (locked) container in a secured area to prevent SBU data from unauthorized disclosure or access.
- (3) CORs hold responsibility for verifying all contractors keep certification designation with an industry trade association that conducts scheduled and unannounced site inspections and reports out on findings. Refer to Pub 4812 , Contractor Security & Privacy Controls.

10.5.1.6.10.7
(09-15-2023)
**Recycling Disposition
and Destruction**

- (1) Do not place paper documents with SBU data in regular recycling containers. Instead, place them in clearly marked secured containers (sensitive document destruction bins).
- (2) The preferred approach is to segregate and shred sensitive information following guidelines contained in IRM 10.5.1.6.10, Disposition and Destruction, before turning it over to the recycler.
- (3) Another method is to have IRS personnel observe the destruction of sensitive information upon delivery to the recycler. This allows for destruction of sensitive information while keeping custody of the material up to the moment of destruction. Again, the contractor must follow IRC 6103(n) requirements which provides for safeguards and periodic safeguard reviews.

10.5.1.6.11
(09-15-2023)
**Global Positioning
Systems (GPS) and
Location Services**

- (1) Policy for personally owned GPS device usage and location services (geolocation) on devices balances the business needs of field employees voluntarily using these devices and the privacy and security concerns related to the SBU data that might be in the devices. The purpose of the following is to minimize the risk of exposing SBU data and to prevent unauthorized disclosures. [IRC 6103, Privacy Act]

10.5.1.6.11.1
(05-08-2025)
**Global Positioning
Systems (GPS)**

- (1) This exception for the use of personally owned GPS devices is limited to GPS functions only. For example, this does not apply to the use of the non-GPS functions on personally owned mobile computing devices.
- (2) Input only taxpayer address information into the GPS device and delete this information from the device once no longer necessary. Never input individual or business taxpayer names into the device.
- (3) Do not connect the GPS device to an IRS computer, as the device has the potential to introduce computer viruses and malware into the IRS network.
- (4) If available, use a security personal identification number (PIN) code with the device to help protect the privacy of tax information in case the device is lost or stolen.
- (5) Do not leave the GPS device unattended or unsecured.
- (6) Remove portable GPS devices from the vehicle when not in use as circumstances allow. In those limited times where you must leave a portable device in a locked vehicle, store it out of sight in the trunk or glove compartment.
- (7) Never leave portable GPS devices in a vehicle overnight.
- (8) Do not leave the portable GPS device and any mounts in an unattended vehicle in plain sight. After removing the mount, clean the suction cup mount area because it can leave marks on the windshield or dashboard showing that a GPS or other device may be present in the vehicle, increasing the risk of a break-in.
- (9) Report the loss or theft of a GPS device with taxpayer addresses (whether a government-issued GPS or a personally-owned GPS), as a potential data breach of PII:

- a. Immediately upon discovery of the loss or theft, the employee must report the potential data breach to the employee's manager and the proper organizations based on what was lost or disclosed.
- b. For more information about how to report an incident and data breach, refer to IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures, or the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.

10.5.1.6.11.2
(09-15-2023)

Location Services

- (1) Except for the use of a GPS in IRM 10.5.1.6.11.1, Global Positioning Systems (GPS), we strongly encourage you not to use your personal devices (such as phones, tablets, fitness watches, or wearable devices) or applications on them to identify taxpayer or work addresses with location services (geolocation), geotagging, or GPS features of any social media accounts (such as Facebook Check In™ or Find My Friends™). Geotagging pinpoints location, which might inadvertently reveal a taxpayer's home or business, or show activities and location at an IRS office. You should use an IRS-furnished device (if issued) when finding and receiving directions to taxpayer addresses.

Caution: This includes infectious disease exposure notification applications built into your phone.

- (2) When using services that need location, try to avoid using an exact taxpayer address if it might pinpoint the IRS has an interest in the taxpayer.

10.5.1.6.12
(05-08-2025)

Telework

- (1) Special privacy concerns arise in the telework environment. Like all IRS personnel, teleworking personnel have a responsibility to safeguard SBU data (including PII and tax information). Unique potential risks, such as family members accidentally taking case files left out on a desk, or overhearing phone calls with tax information, create the need for more guidelines.

Note: Remote work and other non-office programs also follow the procedures in this subsection.

- (2) Except for those documents received in a field environment, do not take high security items (review IRM 10.5.1.2.11, High Security Items) to a telework location. [Telework Enhancement Act of 2010; Treasury Telework Program policy, TN-18-001; OMB Guide to Telework in the Federal Government; NIST 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security]
- (3) For more information on telework requirements, refer to IRM 6.800.2, IRS Telework Program.
- (4) For telework mail procedures, refer to IRM 6.800.2.3.4.7, Mail, and IRM 1.22.5.11, Guidance on Telework Employee Mail.
- (5) Be aware of your environment as you conduct business at an approved telework location.
- (6) When setting up a home office, you should evaluate the nature of your work and the level of sensitivity around the information you handle on a day-to-day basis, refer to IRM 6.800.2.3.2, Equipment.

- (7) Do not use an unsecured wireless access point (wi-fi hotspot) as a regular telework location. For more information about secured wireless access points (wi-fi hotspots), refer to IRM 10.8.1.4.1.17, AC-18 Wireless Access.

Note: If you use a hotspot temporarily (not as a permanent telework solution), you must secure it with a password. Refer to the *internal How to use your iPhone as a hotspot site*. Make sure you only use secured wi-fi networks when working at your appointed worksite (approved telework location or approved lodging) and follow this guidance for protecting taxpayer's privacy and safeguarding confidential information.

- (8) Teleworking personnel should follow the following guidelines. For bargaining unit employees, should any of the guidelines conflict with a provision of a negotiated agreement, the agreement will prevail. Individual office practices may supplement this information.

- (9) Teleworking personnel should:

- a. If possible, set home office appointed workspace apart from the rest of the house, ideally with a door you can secure.
- b. Avoid frequent interruptions or working within listening distance of others.
- c. Apply the Clean Desk requirements to data left out in work areas, credenzas, desktops, fax, copy machines, and in or out baskets. When away from the desk, secure SBU data in a locked room, locked file cabinet, or a locked desk, per IRM 10.5.1.5.1, Clean Desk Policy.
- d. When possible, conduct phone conversations in private settings or in locations that minimize the potential for eavesdropping. Hold telephone calls that include audible SBU data within a closed office environment or out of the listening range of others. Review the IRM 10.5.1.6.7.1, Cell Phone or Cordless Device, and IRM 10.5.1.6.20, Smart Devices.
- e. To properly send SBU data, follow IRM 10.5.1.6.9, Other Forms of Transmission, and its subsections, for field and travel, mailing, shipping, electronic, faxing, printing, and phone. This includes securely transporting SBU data to the office for shredding.
- f. If possible, minimize the printing of SBU data to what is explicitly necessary.
- g. To properly dispose of SBU data, review IRM 10.5.1.6.10, Disposition and Destruction.
- h. Bring all SBU data for destruction into the office for proper disposition.

Note: For more information, refer to the *internal Telework Privacy Considerations site*.

10.5.1.6.13
(05-08-2025)
**Bring Your Own Device
(BYOD)**

- (1) Bring Your Own Device (BYOD) is a concept that allows personnel to use their personally-owned technology devices to stay connected to, access data from, or complete tasks for their organizations. At a minimum, BYOD programs allow users to access employer-provided services and data on their personal tablets or smartphones.
- (2) To protect the privacy of the tax information, BYOD participants must:
- (3) Use only IRS-approved applications.
- (4) Refrain from using devices in public settings where others might overhear conversations involving SBU data (including PII and tax information) or where

others might review screens with this information. Review IRM 10.5.1.6.7.1, Cell Phone and Cordless Device.

- (5) Follow the terms in the Personally-Owned Mobile Device Acceptable Use Agreement, including:
 - Report lost or stolen devices promptly and accurately.
 - Follow procedures for removal of the IRS-approved mobile device business software if changing your device or leaving the program.
 - Follow all applicable laws, regulations, rules, policies, and procedures, including Federal Records Act, Office of Government Ethics Standards of Ethical Conduct, and the Department of the Treasury Employee Rules of Conduct.
- (6) The BYOD program protects privacy. All BYOD users must acknowledge: **Use of this system constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities** on the IRS-approved mobile device business software on their mobile devices. Refer to IRM 10.8.1.4.1.7, AC-08 System-Use Notifications.
- (7) For your privacy, you may block the outgoing phone number of the personal device per the *internal BYOD site*.

Note: The Fair Debt Collection Practices Act (FDCPA) does not prohibit this practice by the IRS. The IRS is not a creditor or debt collector under the FDCPA. Section 803 (6) of the FDCPA defines the term “debt collector,” and specifically excludes in (C) “any officer or employee of the United States or any State to the extent that collecting or attempting to collect any debt is in the performance of his official duties.”

- (8) Refer to IRM 10.8.26, Wireless and Mobile Device Security Policy, and IRM 10.8.27, Personal Use of Government Furnished Information Technology Equipment and Resources.

10.5.1.6.14 (05-08-2025) Civil Liberties

- (1) Privacy and civil liberties often overlap.
- (2) Civil liberties are the rights of people to do or say things that are not illegal without the government stopping or interrupting them (due process). For example, the U.S. Constitution’s *Bill of Rights (external)* guarantees civil liberties.
- (3) The Privacy Act provides for privacy and civil liberties protections, outlined in IRM 10.5.1.6.14.1, First Amendment, and detailed in IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections).
- (4) 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 are responsible for being familiar with and acting in accord with taxpayer rights. Refer to IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For more information about the TBOR, refer to the *Taxpayer Bill of Rights (external)*. The TBOR requires the IRS to protect taxpayer rights to privacy (with due process) and confidentiality as essential rights that help protect their civil liberties.
- (5) The Privacy Act also allows for due process rights, as it forms the basis for the IRS Privacy Principles.

- (6) Many existing privacy policy and compliance requirements, including the IRS Privacy Principles, also protect civil liberties. For example, the principle of Data Quality ensures fair treatment. The principle of Access, Correction, and Redress ensures due process, as do the principles of Openness and Consent, and Verification and Notification.
- (7) The IRS further addresses civil liberties protections through the PCLIA. The PCLIA reinforces Privacy Act requirements for the collection of First Amendment activities information and monitoring of individuals (review IRM 10.5.1.6.14.3, Monitoring Individuals). [RA-08]
- (8) Refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA), for more information on the PCLIA process.
- (9) For more information, refer to IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections).
- (10) For more information, refer to *TD P 25-04 Privacy Act Handbook (pdf)(external)*, Record Keeping Under the Privacy Act.

10.5.1.6.14.1
(09-15-2023)
First Amendment

- (1) The Privacy Act prohibits federal agencies from maintaining records on how any individual exercises their First Amendment rights unless certain exceptions apply. [Privacy Act; Purpose Limitation; PT-07(2)]
- (2) First Amendment rights include religious and political beliefs, freedom of speech and of the press, and freedom of assembly and petition.
- (3) Congress intended agencies to apply the broadest reasonable interpretation when determining whether an activity is a right guaranteed by the First Amendment.
- (4) IRS personnel must not keep files of persons who are merely exercising their constitutional rights.
- (5) IRS personnel involved in the design, development, operation, or maintenance of any system of records subject to the Privacy Act must be aware of the restrictions on keeping records on the exercise of First Amendment rights and alert to any potential violation of those restrictions.
- (6) Taxpayers must report income and provide information necessary to verify deductions on their tax returns. The IRS may collect such information although, sometimes, this data may reveal how individuals exercise their First Amendment rights, such as religious affiliation, group membership, or political preference. The IRS may collect this information because statutory exceptions apply.
- (7) For more information, refer to IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections).

10.5.1.6.14.2
(05-08-2025)
Recordings in the Workplace

- (1) Widely available electronic recording and monitoring technology (such as online meetings, digital cameras, smartphones, and smart devices) raises privacy and security concerns.
- (2) Privacy concerns for recording (including audio, video, transcription, photographic, or infrared) in the workplace or while conducting official business center around individual employee privacy, the potential disclosure of SBU

data (including PII and tax information), data minimization, and federal records creation and retention. [Minimizing Collection, Use, Retention, and Disclosure]

Note: These recordings will be federal records and subject to FOIA and Electronic Discovery. For more information about where these federal records must reside, refer to IRM 1.15.6, Managing Electronic Records.

- (3) The law for recording others varies by state, but many states require consent of both the recording individual and the recorded individual. To protect individual employee privacy, IRS policy prohibits most recordings because of such variations. IRC 7521 applies to recording taxpayer interviews, as described in the business need paragraph IRM 10.5.1.6.14.2 (6).
- (4) Personnel must not electronically create or share audio or video recordings or transcriptions of conversations, meetings, or conferences in the workplace or while conducting official business, except where authorized. *[31 CFR 0.215, Recording Government Business] (external)*
- (5) If you must record in the workplace, you need these elements for authorized recording:
 - a. Business need [Minimizing Collection, Use, Retention, and Disclosure] — review IRM 10.5.1.6.14.2 (6).
 - b. Approval [Accountability] — review IRM 10.5.1.6.14.2 (7).
 - c. Consent [Openness and Consent] — review IRM 10.5.1.6.14.2 (8).
 - d. Precautions [Strict Confidentiality] — review IRM 10.5.1.6.14.2 (9).
 - e. Government-furnished equipment (GFE) or government-approved equipment [Security; Minimizing Collection, Use, Retention, and Disclosure] — review IRM 10.5.1.6.14.2 (10).
- (6) **Business need:** Minimize recordings in the workplace unless you have a compelling business need. Just recording to refresh your memory after a meeting for easier notes is not a compelling business need to record. Examples of compelling business needs that allow for limited recording in the IRS workplace with approval and consent include:

Business need	Explanation
Service quality control:	You may make recordings to document or verify the quality of service, such as with contact recording.

Business need	Explanation
Taxpayer interviews:	<p>In limited cases, taxpayers may request to audio record in-person interviews, with prior notice to the IRS, and the IRS may record those interviews, under IRC 7521(a). The IRS may also initiate audio recordings of taxpayer interviews. Refer to IRM 4.10.3.4.7, Requests to Audio Record Interviews; IRM 5.1.12.3, Recording Taxpayer Interviews; and IRM 25.5.5.4.4, Right to make an Audio Recording of the Proceeding.</p> <p>Caution: Taxpayers do not have the right to record phone (including online meeting) interviews. If you know a party other than the IRS is recording a taxpayer call (such as a prison recording an incarcerated taxpayer), end the call as described in IRM 21.1.3.17.3, Taxpayer Request to Tape Record Conversation.</p>
Investigation:	<p>This policy does not apply to criminal investigations or official investigations relating to the integrity of any officer or employee of the IRS. Refer to IRC 7521(d).</p>
Employee education:	<p>When used for employee education, employees may make recordings using IRS-issued software applications or platforms, such as Adobe Articulate™, or Teams™.</p>
Required attendees unavailable:	<p>When required personnel are unavailable (such as for a demonstration of a tool), organizers may record for missing personnel.</p>
Reasonable accommodation:	<p>When performed by an individual with a disability as part of an approved reasonable accommodation, certain recordings may be allowed. Refer to IRM 1.20.2, Providing Reasonable Accommodation for Individuals with Disabilities.</p>
Labor relations:	<p>The policy is not intended to and should not be interpreted to interfere with employee rights to engage in concerted activity under the National Labor Relations Act. For more information, refer to IRM 6.432.1, Addressing Poor Performance; IRM 6.711.1, Authorities, Responsibilities, and Processes; IRM 6.751.1, Discipline and Disciplinary Actions: Policies, Responsibilities, Authorities and Guidance, IRM 6.752.1.7, Employee Entitlements; and IRM 6.771.1.5, Employee Coverage.</p>

Note: These recordings will be federal records. For more information about where these federal records must reside, refer to IRM 1.15.6, Managing Electronic Records.

(7) Approval:

- a. For IRS-initiated audio recordings with taxpayers, Field Territory manager approval is required. Refer to IRM 4.10.3.4.7, Request to Record Audio Interviews.
- b. For physical security reasons, IRS personnel must not conduct photography or video recordings without prior FMSS approval in IRS facilities. Refer to IRM 10.2.14.6, Photography and Video Recordings Prohibition.
- c. While you do not need approval at alternative duty stations (such as satellite locations, employee's residence), for privacy and security reasons, you still must not record SBU data, except where allowed in this policy. Refer to IRM 10.8.1.4.1.18.2, Video and Photographic Technologies.

Exception: Audio recordings outside of online meetings require direct supervisor approval. Online meeting audio and video recordings do not require approval, unless otherwise specified by a business unit procedure.

- (8) Consent:** If you must record, get consent to record from all participants. For example, before you record, announce why you need to record and ask for consent. They can give explicit consent (verbal or by other action) or give implied consent after notice of recording by staying on the call or in the meeting. If you intend to disclose the recording for a legitimate business need, get written consent, such as via Form 15293, Consent for Disclosure of Non-Tax IRS Records Protected under the Privacy Act. Refer to IRM 10.5.6.2.3, Privacy Act Consent to Disclosure. For photo or video in IRS publications, use Form 14483-A, Model/Photo Release, instead of Form 15293, Consent for Disclosure of Non-Tax IRS Records Protected under the Privacy Act.

Exception: If someone who has refused consent or not consented makes threats via telephone, the employee may start emergency recording because: a) federal law authorized the employee's conduct and b) the employee's conduct was "reasonable and necessary" to carry out their duty. [Supremacy Clause of U.S. Constitution, art. VI, cl. 2] Refer to IRM 21.1.3.10.3, Assault/Threat Incidents/Abusive Caller; IRM 21.1.3.10.7, Bomb Threats; and IRM 21.1.3.12, Suicide Threats.

(9) Precautions:

- a. Take precautions that no unauthorized recordings or disclosures occur.
- b. Limit SBU data (including PII and tax information) in recordings.
- c. If you must include SBU data, mark it as such. If audio or video, announce at beginning of recording that it will include sensitive content that only those with a need to know can access. This helps identify sensitive content if reviewed for audit, litigation, or FOIA requests. Review IRM 10.5.1.6.5, Marking.
- d. When working on any form of SBU data (including PII and tax information), such precautions include muting or disabling voice-activated devices and smartphone applications (such as FaceTime™, Siri™ or Google Now™ ("Okay Google")) on devices). For more information about precautions, review IRM 10.5.1.6.20, Smart Devices, about digital assistants, smart devices, IoT, and other devices that can record or send sensitive audio or visual information.

- e. If you receive proper approval and consent to make a recording or take a photograph, you must not record or photograph unnecessary SBU data (including PII and tax information). Make sure those items are not in view or earshot of the device.
- f. If SBU data (including PII and tax information) appears in an electronic recording nonetheless, you must protect the recording as SBU data and must not disclose the information unless a statutory exemption applies under IRC 6103 or the Privacy Act (depending on the nature of the data).

- (10) **Government-furnished or government-approved equipment:** Use GFE or approved equipment (including BYOD) to record. Contractors must not record on non-government equipment, even if they have not been issued IRS equipment. Have an IRS employee record if necessary. Refer to IRM 10.8.2.3.1.18, Contractor.

10.5.1.6.14.3
(12-31-2020)

Monitoring Individuals

- (1) The IRS needs to conduct some monitoring of individuals to protect federal systems, information, and personnel. Examples of such monitoring include access logs to IRS facilities and audit trails that monitor IT usage. [Privacy Act; PE-08(3)]
- (2) Limitations still exist on use of any PII collected, with sharing on a need-to-know basis for its intended use only. [Privacy Act; AU-03(3)]
- (3) Monitoring of the public outside IRS facilities must not occur without first consulting Privacy Policy [Treasury's Privacy and Civil Liberties Impact Assessment Template and Guidance]. For help, email **Privacy*.

Note: This policy does not apply to criminal investigation activities. Refer to IRM 9.4.6, Surveillance and Non-Consensual Monitoring.

- (4) For more information about the limitation of monitoring individuals, refer to IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections).
- (5) The IRS PCLIA addresses these limitations. For more information about PCLIAs, refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA). Contact **Privacy Review* for questions. [RA-08]

10.5.1.6.15
(05-08-2025)

Contracts

- (1) The IRS defines personnel to include contractors in IRM 10.5.1.1.2, Audience. Contractors and applicable IRS personnel must follow the requirements in IRM 10.5.1.4.1, Employees and Personnel, and IRM 10.5.1.4.7, Personnel in Contract Activities.
- (2) The IRS has statutory and regulatory privacy obligations for contracts. To meet these obligations, the Chief Privacy Officer (CPO) as designee of the Senior Agency Official for Privacy (SAOP), must make sure the IRS [Privacy Act, IRC 6103(n), OMB A-130, NIST, Accountability]:
 - a. Establishes privacy roles, responsibilities, oversight, and access requirements for contractors and service providers throughout the privacy lifecycle.
 - b. Includes privacy requirements for all relevant stages of the privacy lifecycle in contracts and other contract-related documents, including end of contract.

- c. Follows Privacy Act and IRC requirements for contracts, outlined in IRM 10.5.6.2.9.1, Privacy Act Contract Requirements, and IRM 11.3.24.2, Requirements.
- (3) The IRS CO, COR, and others responsible for contract-related activities must meet the requirements in the subsections outlined in the following table, if they apply to their respective roles:

IRM	Title
IRM 10.5.1.4.7	Personnel in Contract Activities
IRM 10.5.1.6.15.1	Contract Privacy Requirements Language
IRM 10.5.1.6.15.2	Contracting Officer's Representative (COR) Training
IRM 10.5.1.6.15.3	OneSDLC in Contracts
IRM 10.5.1.6.15.4	Privacy Act in Contracts
IRM 10.5.1.6.15.5	IRC 6103 (Tax Information) in Contracts
IRM 10.5.1.6.15.6	Background Investigation
IRM 10.5.1.6.15.7	Mandatory Training for Contractors
IRM 10.5.1.6.15.8	Non-Disclosure Agreements
IRM 10.5.1.6.15.9	Privacy and Security Controls in Contracts
IRM 10.5.1.6.15.10	Privacy and Civil Liberties Impact Assessment (PCLIA) in Contracts
IRM 10.5.1.6.15.11	Testing and Development Environments in Contracts
IRM 10.5.1.6.15.12	Incident Response in Contracts
IRM 10.5.1.6.15.13	Unauthorized Access (UNAX) in Contracts
IRM 10.5.1.6.15.14	Contract Closeout
IRM 10.5.1.6.15.15	Federal Acquisition Regulation (FAR) Compliance
IRM 10.5.1.8.9.2	PL-4 Planning – Rules of Behavior [J] {Org}
IRM 10.5.1.8.10.13	PM-17 Program Management – Protecting Controlled Unclassified Information on External Systems [J] {Org}
IRM 10.8.1.4.14.1	PS-02 Position Risk Designation
IRM 10.8.1.4.14.2	PS-03 Personnel Screening (InTC)
IRM 10.5.1.8.11.1	PS-6 Personnel Security – Access Agreements [J] {Org}
IRM 10.5.1.8.14.3	SA-04 System and Services Acquisition – Acquisition Process [J] {Sys}

- (4) In this IRM, contract privacy requirements apply to contractors, subcontractors, contractor employees, and subcontractor employees. Contract requirements

flow down to subcontracts (which the IRS must approve) under the *internal IRS Acquisition Policy (IRSAP) site Index C (pdf)*.

- (5) For more procurement information, refer to the *internal Office of the Chief Procurement Officer Customer Portal*.
- (6) For more privacy information, refer to the *internal contracts site*.
- (7) For help with privacy contract requirements, email **Privacy*.

10.5.1.6.15.1
(05-08-2025)

**Contract Privacy
Requirements Language**

- (1) All IRS contracts, with few approved exceptions, must include the entire current version of the SBU data privacy requirements language (formerly contract clauses) found on the *internal IRS Acquisition Policy (IRSAP) site Index C (pdf)*:
 - a. Submission of Security Forms and Related Materials (formerly IR1052.204-9000)
 - b. Notification of Change in Contractor Personnel Employment Status, Assignment, or Standing (formerly IR1052.204-9001)
 - c. Safeguards Against Unauthorized Disclosure of Sensitive but Unclassified Information (formerly IR1052.224-9000)
 - d. Mandatory IRS Security and Privacy Training for Information Systems, Information Protection and Facilities Physical Access (formerly IR1052.224-9001)

[PM-17; SA-04]

- (2) The IRSAP requirements provide binding internal policy to the IRS for all IRS acquisitions. The requirements language in a contract legally binds the contractor. Per the IRSAP, the Office of the Chief Procurement Officer (OCPO) must use the IRSAP to make sure contracts follow IRS-specific policy. The IRS must use the IRSAP in conjunction with the DTAP, DTAR, and FAR to make sure contracts follow all Treasury and IRS policies and federal procurement regulations.
- (3) In addition to the SBU data contract requirements language, include in the solicitation, request for proposal, contract, statement of work (or similar document, such as task order, performance work statement, or statement of objectives), and work order [Privacy Act, IRC 6103(n)]:
 - a. Business need and justification for how the contractor will use the data.
 - b. Specific data elements.
 - c. Authorized purpose and use (legal authority that allows us to share the data).
 - d. Who will receive the data.
 - e. How to protect the data at rest and in transit.
 - f. What happens to the data after the need ends.
- (4) Review IRM 10.5.1.6.15.4, Privacy Act in Contracts, and IRM 10.5.1.6.15.5, IRC 6103 (Tax Information) in Contracts.
- (5) For an exception to the requirement to include the privacy requirements language in a contract, you must get approval from privacy. Email your exception request (with documentation) to the **Privacy* mailbox for approval. Include Privacy's approval response in your procurement shopping cart.

- 10.5.1.6.15.2
(05-08-2025)
Contracting Officer's Representative (COR) Training
- (1) Review and understand the proper privacy contract-related training and guidance, including the COR Security, Privacy, and Disclosure Awareness Training. [AT-03(5); PM-17; SA-04]
 - (2) For more information, refer to the *internal COR Community of Practice (CCOP) site*.
- 10.5.1.6.15.3
(05-08-2025)
OneSDLC in Contracts
- (1) Follow the One Solution Delivery Life Cycle (OneSDLC) process. [PM-17; SA-04]
 - (2) For more information about OneSDLC, refer to IRM 2.31.1, One Solution Delivery Life Cycle Guidance, or the *internal OneSDLC site*.
- 10.5.1.6.15.4
(05-08-2025)
Privacy Act in Contracts
- (1) Contract work statements (or similar documents) must specifically name the proper System of Records Notice (SORN) when Privacy Act information is a part of the research, design, development, testing, or operation work under the contract. [PM-17; SA-04]
 - (2) Include the Privacy Act authority, use, protections, and penalties for violations. [PL-04; PS-06]
 - (3) For more information, review IRM 10.5.1.6.15.1, Contract Privacy Requirements Language, and refer to IRM 10.5.6.2.9.1, Privacy Act Contract Requirements.
- 10.5.1.6.15.5
(05-08-2025)
IRC 6103 (Tax Information) in Contracts
- (1) When the contract involves tax information, the contract must include IRC 6103 authority, use, protections, prohibitions on redisclosure (secondary use of data), and penalties for violations. [IRC 6103(n); PM-17; SA-04]
 - (2) For more information, review IRM 10.5.1.6.15.1, Contract Privacy Requirements Language, and refer to IRM 10.5.6.2.9.1, Privacy Act Contract Requirements, and IRM 11.3.24.2, Requirements.
- 10.5.1.6.15.6
(05-08-2025)
Background Investigation
- (1) Support the proper level of contractor background investigation in cooperation with the Office of Personnel Security (PS), Contract Security Onboarding (CSO), per IRM 10.23.2.2.1, Vendor and Contracting Officer's Representative Roles. [PS-02; PS-03; PS-06; PM-17; SA-04]
 - (2) This includes working with PS to assign the correct risk designations (often Moderate for access to SBU data), helping coordinate contractor fingerprinting, and distributing identity cards, if needed.
 - (3) For position risk designations, following IRM 10.23.2.5, Position Risk Designations:
 - a. All contracting actions with SBU data (including PII and tax information), with few exceptions, carry a moderate impact security level as public trust positions.
 - b. Public Trust positions involve access to, operation, or control of proprietary systems of information, such as financial or personal records, with a significant risk for causing damage to people, programs, or an agency, or for realizing personal gain [OPM suitability guidance]. Per Treasury policy, public trust positions are moderate and high risk [TD P 15-71]. Per IRM 10.23.3.6, Investigative Tiers, the minimum investigative require-

ments for IRS public trust positions as recommended by the Department of the Treasury and OPM are: Tier 2 – Moderate Risk and Tier 4 – High Risk.

- c. When assigning a risk designation, you must consider the level of IRS supervision over the individual with access to SBU data. For contractors (especially off-site), their ability to act independently with only occasional review by the IRS limits the level of IRS supervision.
- d. Contracts with staff-like access to FISMA systems carry a High impact security level. These are security impact levels, not background investigation levels. Refer to Pub 4812, Contractor Security & Privacy Controls, the Security Categorization section.

- (4) Any staff-like access (facilities, systems, or SBU data) requires completion of a favorable suitability or fitness determination (background investigation) conducted by IRS Personnel Security.
- (5) If contractors need re-investigation, the COR must start those.
- (6) For the definition of staff-like access, refer to IRM 10.23.2.1, Program Scope and Objectives.

10.5.1.6.15.7
(05-08-2025)
Mandatory Training for Contractors

- (1) Contractors must take required security, privacy, disclosure, and UNAX training within the required time limits per IRM 10.23.2.10, Security Awareness Training (SAT) Requirements, before access and annually thereafter to keep access during the contract. [AT-03(5); PM-17; SA-04]
- (2) To be authorized and to have access to sensitive data, all personnel must have a need to know and must complete required training (IRS annual and role-based privacy, information protection, and disclosure training requirements, UNAX awareness briefings, records management awareness briefing, and all other specialized privacy training) and background investigations before given access to SBU data (including PII and tax information). [OMB A-130]

10.5.1.6.15.8
(05-08-2025)
Non-Disclosure Agreements

- (1) Complete Non-Disclosure Agreements (NDAs) within the required time limits per PS instructions and IRM 10.23.2.17, Non-Disclosure Agreement (NDA) for Access to Sensitive Information. [PL-04; PM-17; PS-06; SA-04]
- (2) All contractors must sign NDAs before receiving access to SBU data (including PII and tax information).

10.5.1.6.15.9
(05-08-2025)
Privacy and Security Controls in Contracts

- (1) Contracts must reference and contractors must follow Pub 4812, Contractor Security & Privacy Controls. [PM-17; SA-04]
- (2) Pub 4812 incorporates requirements from IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls, and the relevant policies in the IRM 10.8 series, Information Technology (IT) Security.

10.5.1.6.15.10
(05-08-2025)
Privacy and Civil Liberties Impact Assessment (PCLIA) in Contracts

- (1) Contractors must receive and understand the PCLIA when supporting a project with a PCLIA. [PM-17; RA-08; SA-04]
- (2) In some cases, contractors might need to work with the IRS to complete the required PCLIA.

- (3) Before developing or procuring information technology that uses PII, the IRS must complete a PCLIA. The IRS requires PCLIA's for systems, pilot projects, research, experimentation, the use of innovative technologies, technical demonstrations, prototypes, and proof of concepts, surveys, and the like. [E-Government Act]
 - (4) For more information about the PCLIA process, refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA) and the *internal PCLIA site*.
- 10.5.1.6.15.11
(05-08-2025)
Testing and Development Environments in Contracts
- (1) Contracts involving the use of SBU data in testing and development environments must follow the requirements of IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments. [PM-14; PM-17; SA-04]
 - (2) For more information, refer to the *internal SBU Data Use Process site*.
- 10.5.1.6.15.12
(05-08-2025)
Incident Response in Contracts
- (1) Make sure the contractor understands incident and data breach response and their timely reporting requirements. [IR-02 through IR-08; PM-17; SA-04]
 - (2) Immediately report all incidents and data breaches related to IRS processing, information, or information systems upon discovery to the CO and COR.
 - (3) Per IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures, contractors must refer to the *Contractor Security Information page on IRS.gov (external)* and Pub 4812, Contractor Security and Privacy Controls, for information about contractor incident and data breach response and reporting procedures.
- 10.5.1.6.15.13
(05-08-2025)
Unauthorized Access (UNAX) in Contracts
- (1) Report unauthorized access (UNAX) by a contractor to TIGTA, the CO, and COR. [IR-02 through IR-08; PM-17; SA-04]
 - (2) For more information on UNAX, review IRM 10.5.1.2.5, UNAX, and refer to IRM 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements, and the *internal UNAX site*.
- 10.5.1.6.15.14
(05-08-2025)
Contract Closeout
- (1) Begin the closeout process in time to complete closeout before the contract ends to maintain proper protection and control of SBU data. [MP-06; PM-17; SA-04]
 - (2) Collaborate with Contractor Security Management (CSM) at contract closeout to revoke system and facilities access.
 - (3) Contractors and those responsible must return all IRS data or dispose of it as required by the contract.
 - (4) Refer to the IRM 1.15 series, Records and Information Management, to follow paper and electronic records management requirements.
- 10.5.1.6.15.15
(05-08-2025)
Federal Acquisition Regulation (FAR) Compliance
- (1) Follow the Federal Acquisition Regulations (FAR) for all contracts. [PM-17; SA-04]
 - (2) For more information, refer to the *FAR (external) site*.

10.5.1.6.16
(05-08-2025)
**Online Data Collection
and Privacy Notices**

- (1) Online data collection may require several kinds of notices, such as:
 - a. An IRS-approved IT system use notification message (refer to IRM 10.8.1.4.1.7, AC-08 System-Use Notifications).
 - b. Link to IRS.gov Privacy Policy (review IRM 10.5.1.6.16.1).
 - c. An online data collection Privacy Act statement (review IRM 10.5.1.6.16.2).
 - d. Privacy departure notice (review IRM 10.5.1.6.16.3).
- (2) When building an online form that allows unrestricted input by users, tell the user whether it is secure for personal information.

Example: If your form is in an unauthenticated chat, add a banner that says: Do not input sensitive personal information, such as your social security number.

- (3) Do not use persistent cookies or other tracking devices to monitor the public's visits on an IRS internal or publicly accessible website, except as authorized by OMB regulations. [OMB M-03-22]
- (4) After following the guidance in this subsection for writing your notice, Privacy Policy must review and approve the final notice. For approval or questions, email **Privacy*.

10.5.1.6.16.1
(05-08-2025)
**IRS.gov Privacy Policy
Notice**

- (1) The overarching, general IRS internet privacy policy notice at *IRS.gov/privacy (IRS Privacy Policy page)(external)* informs the public of the information collection procedures and the privacy measures in place for its public-facing websites and digital services. It gives useful information that the public would need to make an informed decision about whether and how to interact with the IRS online. [OMB M-23-22; OMB M-10-23; E-Government Act; OMB A-130; OMB M-03-22; Openness and Consent; PM-20; PT-05]

Note: OMB M-23-22 defines digital service as “a transactional service (such as an online form or account management tool) or an informational service delivered over the internet across a variety of platforms, devices, and delivery mechanisms (such as mobile applications or text and short message service (SMS)).” In this IRM, the term includes online applications, systems, programs, databases, and other kinds of interactive information technology.

- (2) Link to the *IRS Privacy Policy page (external)* at every major entry point to all IRS public-facing websites and digital services, as well as on any page collecting personal information from the public. If your public-facing website or digital service collects different information than listed on the IRS Privacy Policy, you also must include a unique online Privacy Act statement. Review IRM 10.5.1.6.16.2, Online Data Collection Website or Application Privacy Policy Notice. [OMB M-23-22, OMB M-03-22]
- (3) The PGLD Privacy Policy office maintains the language for the IRS Privacy Policy, which also serves as the IRS Privacy Program page.
- (4) The OMB requires the following for an agency's privacy policy page, as shown by the *IRS Privacy Policy page (external)*:

Requirements for agency privacy policy page	OMB reference
Give an overview of IRS privacy practices.	M-03-22
<p>Explain the general nature of any PII the IRS collects online, including:</p> <ul style="list-style-type: none"> • What we collect. • Authority to collect. • Purpose of collection (why). • Use of PII (how). • Consent (whether voluntary and how to grant consent). <p>Note: For more specific PII collections, the website or digital service must include an online Privacy Act statement that includes those required elements. Review IRM 10.5.1.6.16.2, Online Data Collection Privacy Act Statement. [OMB M-03-22]</p>	M-03-22
Describe any information collected and stored automatically by the system and how the IRS uses this information.	M-03-22
Identify when the IRS uses tracking technology, its purpose, and the option to decline it.	M-03-22
Note that security and intrusion protection measures are in place.	M-03-22
Organize in a way that is easy to understand and navigate in plain language.	M-23-22
Include useful information that the public would need to make an informed decision about whether and how to interact with the agency.	M-23-22
<p>Describe use of third-party websites and applications, including:</p> <ul style="list-style-type: none"> • Purpose of their use. • Use of PII that becomes available through them. • Other privacy risks and mitigations. • Links to their relevant privacy policies when feasible. 	M-10-23
Show updated substantive changes to the practices it describes.	M-23-22
Date stamp to inform users of the last time the agency made a substantive change to the practices the privacy policy describes.	M-23-22
Make machine-readable.	M-03-22
Follow all other applicable OMB requirements.	M-23-22
<p>Outline rights under the Privacy Act [OMB M-03-22], via a link to the agency's privacy program page, which must list link to:</p> <ul style="list-style-type: none"> • System of Record Notices (SORNs). • Privacy Impact Assessments (PIAs), which at the IRS are Privacy and Civil Liberties Impact Assessments (PCLIAAs). • Matching notices and agreements. • Exemptions to the Privacy Act. • Privacy Act implementation rules. • Publicly available agency policies on privacy (<i>IRS Privacy Policy (external)</i>). • Publicly available agency reports on privacy. • Instructions for sending a Privacy Act request. • Contact information for sending a privacy question or complaint. • Contact information for the Senior Agency Official for Privacy (SAOP). 	<p>M-03-22 M-23-22 A-108</p>

10.5.1.6.16.2
(05-08-2025)
**Online Data Collection
Privacy Act Statement**

- (1) The Privacy Act requires a statement when an agency asks individuals to supply information that will become part of a system of records under the Privacy Act. If online, it must appear at the point of collection or via a link to the agency's privacy policy notice. [OMB M-23-22, OMB M-03-22]
- (2) A unique Privacy Act statement for a public-facing website or digital service must include a link to and detail any differences from the *IRS Privacy Policy (external)*. This statement must appear at the point of collection, which means at the entry point where the data collection differs from the *IRS Privacy Policy (external)*. While the *IRS Privacy Policy (external)* serves as an overarching general notice, your website or digital service needs to tell the public what different information you collect. It serves as the online version of the Privacy Act notice described in IRM 10.5.6.4.2, Notice to Individuals Asked to Supply Information (Privacy Act Notice). This policy applies to any public-facing website or digital service hosted by or for the IRS. [Privacy Act, OMB M-23-22, OMB M-10-23, E-Government Act, OMB A-108, OMB A-130, OMB M-03-22, Openness and Consent, PT-05, PT-05(2)]

Note: For internal websites or digital services, review IRM 10.5.1.6.16.4, Internal Websites and Digital Services Privacy Policy and Privacy Act Statement.

- (3) For a template of a Privacy Act statement with the required elements, refer to IRM 10.5.6.4.2, Notice to Individuals Asked to Supply Information (Privacy Act Notice).
- (4) If your website or digital service is more complex, you might need a more detailed Privacy Act statement than the template.
- (5) After following this guidance for writing your Privacy Act statement, send your draft to Privacy Policy, who must review and approve your notice. For approval or questions, email **Privacy*.

10.5.1.6.16.3
(05-08-2025)
Privacy Departure Notice

- (1) Any IRS internal or publicly accessible website that links to external sites that are not part of an official government domain must label or distinguish non-governmental content, including links to third party websites. This label, also known as a privacy departure notice, alerts visitors that they are about to leave the IRS website and its privacy practices. [OMB M-23-22, OMB M-10-23, Openness and Consent, PT-5]

Note: OMB does not require privacy departure notices for sites that are part of an official government domain, but for transparency and to keep public trust, we recommend that all links to external sites use a privacy departure notice.

- (2) The IRS addresses this by:
 - Publishing a notice to visitors on IRS.gov.
 - Using an external link label such as **(external)** or the icon described in *Links to other websites page (external)*, which meets requirements in *U.S. Web Design System (USWDS) (external)*.

Note: For internal sites, content owners show a link to an external site by adding either the external link label above or “(external)” to the link name, or some similarly clear indicator. For example, a

Knowledge Management site may link to the IRS legal research tool using a link that looks like this: *Bloomberg Law Research (external)*.

10.5.1.6.16.4
(05-08-2025)
**Internal Websites and
Digital Services Privacy
Policy and Privacy Act
Statement**

- (1) The IRS uses the *IRS Internal Privacy Policy and Privacy Act Statement* for internal, non-public facing websites and digital services as a modified version of the *IRS Privacy Policy (external)*. [OMB M-23-22, E-Government Act, OMB M-03-22, Openness and Consent, PT-05(2)]
Note: While not required to post such a policy notice on internal websites, we give this notice to personnel as a privacy best practice and to help meet Privacy Act requirements for online collections of PII. [OMB M-03-22, OMB M-23-22]
- (2) The IRS Source home page is the major entry point for every internal IRS site. The *IRS Internal Privacy Policy and Privacy Act Statement* covers internal websites and digital services linked to and from IRS Source. SharePoint sites and pages do not require more specific notices, unless paragraph (3) applies.
- (3) IRS internal digital services also require an online Privacy Act statement if they collect personnel PII. This must be at the point of collection or via a link. [OMB M-23-22] A link to the *IRS Internal Privacy Policy and Privacy Act Statement* meets this requirement for all internal digital services that only collect personnel PII for access and audit trail purposes.
Note: This policy does not discourage privacy notices on internal digital services beyond the *IRS Internal Privacy Policy and Privacy Act Statement*.
- (4) If your internal digital service collects different information than listed on *IRS Internal Privacy Policy and Privacy Act Statement*, you must tell personnel what information you collect in an online Privacy Act statement described in IRM 10.5.6.4.2, Notice to Individuals Asked to Supply Information (Privacy Act Notice). [OMB M-23-22, OMB M-03-22]
- (5) For more information on internal sites, refer to IRM 11.1.4, Content Policies and Standards for Intranet Sites.

10.5.1.6.17
(05-08-2025)
Social Media

- (1) IRS Communications and Liaison is responsible for external communications, and all external communications must come through their office. Refer to IRM 1.1.11.2.2, Social Media Branch.
- (2) Except for approved IRS communicators handling official IRS media initiatives, the IRS does not authorize you to use social media in an official capacity. Refer to the *internal Social Media Guidelines site* and the IRS Rules of Behavior in the *internal Business Entitlement Access Request System (BEARS)*.
- (3) For more information about internet research guidelines, refer to IRM 11.3.21.8, Requirements for Investigative Disclosure, and IRM 11.3.21.12.1, IRC 6103(k)(6) Disclosures by IRS Employees using Social Networking and Other Internet Sites.
- (4) Personal, non-work usage of these social media tools on personal devices must not compromise the confidentiality of IRS SBU data (including PII or tax information) or the integrity of the IRS. Refer to the *internal Social Media Guidelines site*.

- (5) To use any existing IRS social media tools in communications plans or outreach initiatives, business units must use the proper social media authorization form or contact the proper social media platform owner.
- (6) If an IRS organization would like to consider use of a new social media platform, they must send a New Media Use Authorization Form for approval by the IRS Social Media Governance Council, along with a Social Media PCLIA.
- (7) For more information on Social Media PCLIA's, refer to IRM 10.5.2.2.5.3, Social Media PCLIA.

10.5.1.6.18
(12-31-2020)
**Data on Collaborative
Technology and
Systems**

- (1) This policy does not apply to PII the IRS proactively makes available to all personnel on resource sites (including Discovery Directory, Outlook™ (calendar, profile information, and address book), and SharePoint™ or Teams™ site collections), such as names and business contact information.
- (2) Some of the privacy risks associated with collaborative data sites include:
 - a. Data breaches and inadvertent disclosures.
 - b. Unauthorized access of data without a need to know.
 - c. Sharing data without proper permissions or authorizations.
- (3) The data on collaborative data sites require privacy protections. These protections must include:
 - a. Controlling access to the sites (both as a user and as an administrator).
 - b. Controlling what data is shared on the sites.
 - c. Ensuring privacy and security controls are in place.
 - d. Including all protections in IRM 10.8.1.4.18.14, SC-15 Collaborative Computing Devices and Applications.

10.5.1.6.18.1
(05-08-2025)
Shared Calendar

- (1) You may place information that is not SBU data (including PII and tax information) on all calendars without restriction.
- (2) You must not post SBU data (including PII and tax information) on public calendars with uncontrolled access.

Caution: Calendar entries include meetings, appointments, scheduling notes, and reminders. Make sure only those with a need to know have access to the information.

- (3) The following applies any time a business needs to enter some form of SBU data (including PII and tax information) on a shared calendar:
 - a. Assign permissions on the calendar to limit access to only those people with a need to know the information.
 - b. Encrypt any attachments to the calendar with SBU data (including PII and tax information) other than noted in the following subsections.

Note: This encryption policy does not apply to SBU data (including PII and tax information) the IRS proactively makes available to all personnel on resource sites (including Discovery Directory, Outlook™ (calendar, profile information, and address book), and SharePoint™ or Teams™ site collections), such as names and business contact information.

(4) Use this table for other calendar entries:

Calendar entry	Requirements
Business unit calendar meetings or appointments about taxpayers	<ol style="list-style-type: none"> Place on the calendar only a part of the taxpayer's name, the last two digits of the tax year, and any business unit-specific codes that are not sensitive PII (such as a case control number that is not an SSN and not easily linked to a taxpayer by an outside party). The abbreviated name consists of the first four significant characters of the taxpayer entity's name (the name control): <ul style="list-style-type: none"> For individual taxpayers, these significant characters could include the first four letters of the individual taxpayer's last name (for example, John Finch would be FINC, or use the IDRS name control). If the taxpayer's name consists of only four characters or fewer, you may use the entire name. For corporations, partnerships, trusts or other such entities, the first four letters of the entity's name, excluding articles, could be the first four significant letters used (for example, The Quail Company would be QUAI, or Bluebird Foundation would be BLUE).
Calendars for offices with regulatory, investigative, or advocacy responsibilities (docketed case meetings)	<ol style="list-style-type: none"> These requirements apply to calendars for Appeals, Chief Counsel (Counsel), Criminal Investigation (CI), Taxpayer Advocate Service (TAS), and other functions with regulatory, investigative, or advocacy responsibilities. When the subject matter of the meeting is a case docketed in the United States Tax Court or other judicial forum, calendar the meeting as the case name (for example, the name of the taxpayer with case number). Note: This does not violate privacy principles, as the name of the case is public record information. It falls under the judicially created public records exception. (For more information, refer to IRM 11.3.11.12, Information Which Has Become Public Record.) This practice also applies for unsealed CI matters (such as an indictment, where testimony occurred in an open proceeding, or if an official press release is issued). It would not apply for sealed federal court matters.
Calendars for offices with regulatory, investigative, or advocacy responsibilities (taxpayer meetings)	<ol style="list-style-type: none"> Counsel's calendar entry may use a succinct description of the subject matter and include the case control number assigned to the matter in Counsel's management information system (CASE-MIS). For example, a calendar entry for a meeting to discuss whether to pursue enforcement of a summons in the examination of taxpayer A would appear as "Summons enforcement/POSTF-x01234-56." Except for assignments of cases docketed in the U.S. Tax Court (review earlier subsection), this case control number is not public record and not PII that you must encrypt. So long as the shared calendar is accessible only by Counsel employees whose work requires them to know of such meetings, encryption is not necessary. An invitee could then access CASE-MIS to find the identity of the taxpayer. CI may use the Criminal Investigation Management Information System (CIMIS) investigation number. TAS, as well as Counsel to the National Taxpayer Advocate, may use the Taxpayer Advocate Management Information System number plus the first four (4) significant letters of the taxpayer entity's name.

Calendar entry	Requirements
Non-taxpayer-related meetings or appointments	<ol style="list-style-type: none"> a. An entry on the calendar for meetings with external parties doing business with the IRS (Enrolled Agents, for example) that does not concern specific taxpayers, would consist of the name of the external representative, the name of the organization (where proper), and the subject matter of the meeting. b. You may send any meeting-related non-taxpayer-related PII or SBU data in a separate email (with IT-approved encryption) with directions in the calendar invite to look for the separate email. c. Examples of situations where you may use this practice include: <ul style="list-style-type: none"> • Where Counsel hosts informational meetings with external parties, such as trade groups or other professional organizations, in conjunction with its published guidance program. • Where IRS organizations meet with external parties to plan or deliver presentations or for procurement matters. d. You may voluntarily include your personal appointments on the calendar to make sure business appointments do not conflict. e. Supervisors may note absences of direct reports on their calendar to schedule meetings, assign work, and manage their work unit more efficiently. f. Supervisors may not include more information such as the location of those direct reports, but official travel status and telework notations (without addresses) are acceptable supervisor calendar entries. g. Include leave and other personal information on shared group calendars only with the permission of the affected personnel.

10.5.1.6.18.2

(05-08-2025)

Online Meetings

- (1) Online meeting tools include M365 Teams™, Zoom Workplace™, and AdobeConnect™. Use only IRS IT-approved tools as they will have the necessary authorization and protections, such as encryption, so you can do business with necessary SBU data (including PII and tax information) in a secure environment.

Note: The commercial Zoom™ application is not an IRS-approved tool on the Enterprise Architecture.

- (2) You are always responsible for the information you share in online meetings, just as you are responsible for the information you share in a conversation or email.
- (3) IRS-approved encrypted online meeting tools may convey SBU data; apply the principles of authentication, authorization, and need to know.
- (4) When using approved virtual meeting tools with encrypted communication for official IRS business, you must apply these principles:
 - a. **Authentication:** Use your business unit's authentication methods for all parties. Make sure you know who is in your meeting. Remove unidentified parties from the meeting. This would include tools that are not IRS IT-approved for recording or transcribing. Review IRM 10.5.1.2.9, Authentication.
 - b. **Authorization:** Make sure the people on the meeting are authorized to hear or view the information. Review IRM 10.5.1.2.10, Authorization.

- c. **Need to know:** Share SBU data (including PII and tax information) only with those who have a need to know in the meeting or the chat. Review IRM 10.5.1.2.8, Need To Know.

Example: You may normally conduct an online meeting from a private workspace within your home or from an automobile where you are the only occupant without someone overhearing the conversation. You may also conduct a conversation away from passers-by. Be careful not to convey sensitive information that others might overhear.

- d. Announce the sensitivity of meeting content if you will talk about SBU data and remind attendees of need to know.
- e. Keep a clean desk(top): apply the clean desk policy to your computer screen and anything in view of your camera. Close all applications and documents that don't apply to your meeting. Review IRM 10.5.1.5.1, Clean Desk Policy.
- f. Avoid recording or transcribing meetings and limit SBU data. Before recording online meetings, you must have a legitimate business need, consent from all parties, and other precautions, following requirements in IRM 10.5.1.6.14.2, Recordings in the Workplace.
- g. Meeting hosts (organizers, co-organizers) hold responsibility for controlling the meeting environment, such as removing unauthorized parties, muting audio or video when proper to protect privacy, giving notice and getting consent for recording, promoting others as presenters or co-organizers to help moderate the meeting and chat, announcing sensitivity, and setting meeting options (such as presenters and the meeting waiting rooms).

Caution: If someone's voicemail picks up, remove that party from the call to prevent it from recording the meeting.

Caution: Look for added, forwarded, or unfamiliar attendees, especially if the attendee name does not look like an actual person.

- h. Use IRS contact information (such as email or name).
- i. Do not use personal email or device (unless BYOD) to access virtual meeting tools for official IRS business. [PATH]

Note: Training or publicly available information – IRS personnel may send non-case-related content (or information that is not SBU including PII and tax information), including links, to and from personal accounts when IT Security constraints prohibit access. Review IRM 10.5.1.6.8.4, Emails with Personal Accounts.

- (5) To protect your own privacy, keep chats, profile pictures, and background images professional.
- (6) To prevent inadvertent disclosure, verify which chat or meeting window you are using to make sure you do not put SBU data in the wrong conversation.
- (7) For more information about online meeting privacy, refer to the *internal Online Meeting Tools - Privacy Considerations site*.
- (8) For best practices and answers to questions about using M365™ tools, refer to the *internal M365 site*.

10.5.1.6.18.3
(09-15-2023)

**Shared IRS Storage
(OneDrive, SharePoint,
Teams, and Other IRS
Collaborative Sites)**

- (9) Refer to IRM 10.8.1.4.18.14, SC-15 Collaborative Computing Devices and Applications.
- (1) When putting SBU data (including PII and tax information) on shared storage, check to make sure only those with a need to know have access. Sharing data in collaborative data environments (such as a SharePoint™ site, a group or team site in Teams™, or your OneDrive™) might offer valuable benefits with inherent privacy risks. Understanding the risks involved with sharing data on these sites is key to managing those risks with tight access, privacy, and security controls in place. Collaborative environment access controls must limit access using proper site, folder, file, or other permissions.

Note: For external non-IRS sites, review IRM 10.5.1.6.9.7, Electronic and Online.

- (2) Collaborative environment owners also must make sure their users follow rules and protect privacy.
- (3) You are always responsible for the information you share in collaborative environments, just as you are responsible for the information you share in a conversation or email.
- (4) Most IRS collaborative environments no longer require separate PCLIAs beyond those for their underlying systems. If you use a collaborative environment for a complex processing system using custom code and connecting to other systems, it might become a system that requires a separate system PCLIA. Contact **Privacy Review* to ask if you need a system PCLIA.
- (5) For more information, refer to IRM 10.5.2.2.4, System PCLIA.
- (6) For more information, refer to IRM 10.8.1.4.18.14, SC-15 Collaborative Computing Devices and Applications, IRM 10.8.1.4.18.27, SC-28 Protection of Information at Rest, and IRM 2.25.20.5.3, Personally Identifiable Information (PII)/Sensitive But Classified (SBU) Data.

10.5.1.6.18.4
(05-08-2025)

Cloud Computing

- (1) Before contracting for cloud services, address the necessary privacy, records management, and security policies.
- (2) PGLD must approve all procurements of cloud computing services that include SBU data (including PII and tax information) via the Privacy and Civil Liberties Impact Assessment (PCLIA) process (required by OneSDLC). For more information about OneSDLC, refer to IRM 2.31.1, One Solution Delivery Life Cycle Guidance, or the *OneSDLC site*. [RA-08]
- (3) The IRS PCLIA process addresses privacy concerns for IRS systems with SBU data (including PII and tax information) using cloud computing. These issues include:
 - Who is the Cloud Service Provider (CSP)?
 - Who has access to the information at the Cloud Service Provider?
 - Do other CSPs service this CSP (subcontract with), such as performing updates, maintenance, or other services?
 - What is the Cloud Service Provider's Federal Risk and Authorization Management Program (FedRAMP) compliance status?
 - What deployment model (private, hybrid, or public)?
 - Where does the information go?

- Where is it stored, transmitted?
 - How is it secured? What security categorization (low, moderate, high)?
 - How reliable and secure is the audit trail?
 - How will monitoring be done and how often?
 - Does the CSP contract include all required privacy and security contract requirements language, including those for protecting SBU data (including PII and tax information)?
 - How long must the data be kept? When will it be destroyed?
- (4) Use an existing FedRAMP authorized cloud service offering (CSO) unless you have a compelling justification to use a non-FedRAMP authorized alternative CSO. Refer to IRM 10.8.24.3, IT Security Controls.
 - (5) Using a FedRAMP solution does not mean you automatically have met the privacy and security controls. You still must implement the relevant privacy controls and conduct continuous monitoring. [OMB M-24-15]
 - (6) Except for systems principally supporting overseas federal or Treasury personnel or activities, Treasury systems must be located and operated within the U.S. This includes Treasury contractor systems. [TD P 85-01 control SA-04_T.193, SA-04]
 - (7) PGLD and COR must provide written approval to the contractor if allowing them to keep government data outside the U.S.
 - (8) Modify contracts that do not follow privacy and security requirements.
 - (9) For more information on cloud computing issues and cloud deployment models, refer to IRM 10.8.24, Cloud Computing Security Policy, and IRM 10.8.1, Security Policy.

10.5.1.6.19
(09-15-2023)
Training

- (1) Although IRC 6103(h) (1) allows the disclosure of tax information to IRS personnel for tax administration to the extent the individual obtaining that access has a “need to know,” you must avoid the use of tax information in training and fictionalize SBU data where possible. [Minimizing Collection, Use, Retention, and Disclosure; PM-25]
 - a. Using tax information increases the risks of unauthorized disclosure and might subject the IRS to civil unauthorized disclosure actions which might then result in disciplinary actions against the offending employee(s).
 - b. Use of tax information also raises issues about following the IRS Taxpayer Bill of Rights, codified in IRC 7803(a)(3), which requires the IRS to protect taxpayer rights to privacy and confidentiality. While 6103(h) authorizes disclosure when information is helpful in performing tax administration duties, do not use returns and return information for training purposes when hypothetical or fictional cases will serve the training requirements.

Note: Avoiding extra effort is not justification for increasing risk.

 - c. Employee publications, training and presentation materials are publicly available under the Freedom of Information Act and in the FOIA Library on IRS.gov. That makes it critical that all IRS personnel follow published guidelines to prevent the unauthorized disclosure of tax information.
- (2) For more information about fictionalizing data, refer to the Document 13324, Guidelines and Examples for Fictionalizing Domestic Taxpayer Information;

Document 13311, International Name and Address Construction Job Aid; and IRM 6.410.1.3.10, Disclosure Requirements.

- (3) For more information about training material and marking requirements, review IRM 10.5.1.6.5, Marking, and refer to IRM 6.410.1.3.12, Personally Identifiable Information (PII).

10.5.1.6.20
(05-08-2025)
Smart Devices

- (1) Do not allow digital assistants, smart devices, Internet of Things (IoT), and other devices that can record or send sensitive audio or visual information to compromise privacy in the work, telework, field, or travel environment. These devices typically have sensors, microphones, cameras, data storage components, speech recognition, GPS or location options, and other multimedia capabilities. These features could put the privacy of personnel and taxpayers at risk due to the personal information that might be unwittingly disclosed. When working on any form of SBU data (including PII and tax information), follow these rules:

- a. Treat the device as if it were another person in the room because many such devices and applications can record or send data when activated.
- b. When working with sensitive data, to protect privacy, mute or disable the listening or detecting features of the device, so you don't send SBU data to the device or anything to which it is connected.

Note: To mute or disable these features, refer to the manufacturer instructions. For many devices, go to settings or permissions for these features, looking for privacy, Siri™ or Alexa™, microphone, audio, or similar terms.

- c. If the device or application can take photos or record video or sound, then the personnel must not do sensitive work within visual or audio range.

- (2) Examples of these devices or applications include:

- Digital assistants (such as Dot™ or Echo™ hardware using Alexa™ software or HomePod using Siri™.).
- Voice-activated devices and smartphone applications (such as Siri™, Google Now™ (“Okay Google”), or Alexa™ on devices).
- Wearable devices (fitness trackers, smart watches, etc.).
- Non-IRS-approved video-chatting apps (such as FaceTime™ or SnapChat™).
- Internet of Things (IoT) equipment (or devices or systems), which might include appliances, thermostats, vacuums, or lights.
- Internet-connected toys (such as robots and AI toys or educational toys) that might record (video or audio) and transmit.
- Smart TVs or auxiliary audio or visual equipment (if it includes voice activation).
- Operating systems or applications (such as Windows 10™ or Cortana™) that allow voice commands.
- Home surveillance, security, and video or audio: Including webcams on personal devices in the home, security cameras, or microphones.

- (3) For more information about location-related concerns, review IRM 10.5.1.6.11.2, Location Services.

10.5.1.6.21
(05-08-2025)

Biometric Technology

- (1) The use of biometrics raises privacy concerns due to the inherently sensitive nature of biometric information and public perception that they may be unnecessarily surveilled. You can use biometric technology effectively with proper controls.
- (2) Biometric technology is a combination of the use of very sensitive personal information with automated analysis, often performed by artificial intelligence processing. Biometrics include technologies and data such as:
 - a. Facial recognition
 - b. Voice recognition
 - c. Fingerprint analysis
 - d. Behavioral biometrics
 - e. Physical characteristics, such as height, weight, eye color
- (3) NIST provides definitions of biometrics in several publications, linked from their *Glossary (external)*, including:
 - a. *NISTIR 7316 (external)(pdf)*, Assessment of Access Control Systems: The science and technology of measuring and statistically analyzing biological data. In information technology, biometrics usually refers to automated technologies for authenticating and verifying human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements.
 - b. *NIST SP 800-12 (external)(pdf)*, An Introduction to Information Security: A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.
- (4) Any information technology the IRS uses must meet all IRM 10.5.1.3.2, IRS Privacy Principles, and IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls. For biometrics, system owners and authorizing officials must apply the IRS Privacy Principles:
 - a. **Accountability:** Users of biometric data must be accountable for the collection, use, storage, sharing and disposal of that data. Review IRM 10.5.1.3.2.1.
 - b. **Purpose Limitation:** Collect biometrics only for a legitimate IRS purpose. Review IRM 10.5.1.3.2.2.
 - c. **Minimizing Collection, Use, Retention, and Disclosure:** Only collect the amount of biometric data necessary to achieve the IRS business need; limit its use only to that need and dispose the biometric data when no longer needed. Review IRM 10.5.1.3.2.3.
 - d. **Openness and Consent:** Clearly notify individuals before using their biometric data as to how the IRS will use and safeguard it and their options should they choose not to use the application. Review IRM 10.5.1.3.2.4.
 - e. **Strict Confidentiality:** Only allow access to biometric data by individuals with a need to know it. Review IRM 10.5.1.3.2.5.
 - f. **Security:** The especially sensitive nature of biometric data requires proper security safeguards in place to protect against unauthorized collection, use, disclosure or destruction of the data. Review IRM 10.5.1.3.2.6.
 - g. **Data Quality:** Ensure the accuracy and completeness of biometric data by collecting it directly from the individual to whom it relates. Review IRM 10.5.1.3.2.7.

- h. **Verification and Notification:** When possible, confirm the accuracy of biometric data from the originating source or a reliable, verifiable alternative. Review IRM 10.5.1.3.2.8.
 - i. **Access, Correction, and Redress:** Provide individuals enough information to understand their right to review biometric information the IRS collects and options for participating in maintaining its accuracy. Review IRM 10.5.1.3.2.9.
 - j. **Privacy Awareness and Training:** Provide IRS personnel and vendors who use biometric data with the necessary awareness and training that will guide them to effective privacy decisions. Review IRM 10.5.1.3.2.10.
- (5) System owners and authorizing officials must document how their use of biometrics meets all IRS Privacy Principles and privacy controls in their system's PCLIA and security documentation. For more information about the roles and responsibilities, review IRM 10.5.1.4.4, System Owners, and IRM 10.5.1.4.6, Authorizing Officials (AOs). [RA-08]

10.5.1.6.22
(05-08-2025)

Artificial Intelligence (AI)

- (1) This policy outlines privacy requirements and recommendations to allow for IRS use of artificial intelligence (AI). It applies to IRS users, developers, and providers of AI to follow the Privacy Act and Internal Revenue Code. It links the IRS Privacy Principles, from IRM 10.5.1.3.2, to key AI concepts.

Note: For an overarching IRS AI policy and definition, refer to the *internal Enterprise AI site*.

- (2) All IRS personnel must follow the IRS Privacy Principles to manage risks of AI use.
- (3) IRS privacy policy is technology neutral, meaning that these principles apply to any technology. This policy is for any design, development, acquisition, or use of AI (hereafter referred to as AI use), whether a web-based online form, COTS product or service, custom built IRS tool, or any other use case. This policy applies to associated technology that may not meet the IRS definition of AI. Examples of AI or associated technology include:
- Generative AI
 - Predictive AI
 - Machine Learning (ML)
 - Large Language Models (LLM)
 - Voicebots and chatbots
 - Robotic Process Automation (RPA)

Caution: AI capabilities often appear as part of many other tools, applications or COTS products, without expressly being identified as an AI.

- (4) Use of AI may create new privacy risks or exacerbate privacy risks present in other systems. When using AI, you must consider the relationship between AI and privacy risks, such as collecting more data than is necessary, improper disclosure, misuse, and even aspects of incorrect conclusions that may affect privacy and civil liberties. Use privacy enhancing technologies (PETs), where possible, to protect privacy.
- (5) Use only IRS-approved AI that follow IRS principles and policies for AI risk management, privacy, and security.

- (6) You are responsible for the information you share when using AI, just as you are responsible for the information you share in a conversation or email. This includes considering how the AI might use the information later. Treat AI as another person and follow authentication, authorization, and need to know. Do you know who they are? Are they authorized to review the information? Do they have a need to know? If not, don't share it.
- (7) IRS personnel who manage contracts must make sure that contractors follow this policy. Contractors that use AI must meet all applicable privacy, security, and AI risk management requirements and pass them on to subcontractors.
- (8) System owners and authorizing officials must have written documentation concerning how their use of AI meets all IRS Privacy Principles. The required Privacy Threshold Assessment (PTA) and Privacy and Civil Liberties Impact Assessment (PCLIA), as well as other OneSDLC artifacts, address this documentation. For more information on PCLIAs, refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA).[RA-08]
- (9) The protections required by IRM 10.5.1.8, NIST 800-53 Security and Privacy Controls, also apply to uses of AI.

10.5.1.6.22.1
(05-08-2025)
Accountability for AI

- (1) Under the IRS privacy principle for accountability, IRS users, developers, and providers of AI are responsible for the effective implementation of privacy protections. Whether you are buying or developing a new AI or are the end-user of an application or web service, you must understand how to use the AI so that you protect the information it uses. [Privacy Act sections (e)(9) and (e)(10)]
- (2) IRS personnel who manage contracts must make sure that contractors follow this policy. Contractors that use AI must meet all applicable privacy, security, and AI risk management requirements and pass them on to subcontractors.
- (3) The AI principle from *EO 13960 (external)* of "Responsible and traceable" aligns to the IRS privacy principle of accountability by requiring agencies to clearly define, understand, and assign human roles and responsibilities for AI use. Document and trace these roles, responsibilities and system use plans.
- (4) Review IRM 10.5.1.3.2.1, Accountability.

10.5.1.6.22.2
(05-08-2025)
Purpose Limitation for AI

- (1) Under the IRS privacy principle for purpose limitation, the IRS must only use data for the purpose we originally collected it. Use AI to analyze data only when the analysis supports the need originally described at the time of collection. The purpose may be broad, such as "tax administration," which means the use must align to a defined tax administration purpose. [Privacy Act section (e)(1)]

Example: The IRS can use line-item values to process a tax return (tax administration), but we may also use that data (along with other taxpayers' data) to detect potential noncompliance or fraud (also a tax administration purpose).

- (2) To follow this principle, do not use SBU data (including PII and tax information) to train public AI models.
- (3) The *EO 13960 (external)* AI principle **Purposeful and performance-driven** tells agencies to carefully consider the risks when looking for opportunities for

AI use. Before AI use, the IRS assessment of the risks must include a complete description of the purpose for which we will use the AI and what data the AI uses. By doing a proper risk assessment for your AI, you will limit the use to a legitimate business purpose that can increase the performance of your programs without jeopardizing privacy.

- (4) Review IRM 10.5.1.3.2.2, Purpose Limitation.

10.5.1.6.22.3
(05-08-2025)
**Minimizing Collection,
Use, Retention, and
Disclosure for AI**

- (1) Many AI models can intake, keep, and reuse data. Under the IRS privacy principle for minimization, minimize the collection, use, retention, and disclosure of data in AI to what is specifically relevant and necessary. Take steps to understand how AI might redisclose data and share only what is necessary for your task. When developing an AI model, build in safeguards that guide users how to minimize data and to prevent its improper disclosure. [Privacy Act section (e)(1)]
- (2) To follow this principle, do not use SBU data (including PII and tax information) to train public AI models.
- (3) For more information about disclosure policy, refer to the IRM 11.3 series, Disclosure of Official Information. For more information about reporting incidents and data breaches, refer to IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures.
- (4) The *EO 13960 (external)* AI principle “Lawful and respectful of our Nation’s values” tells agencies to use AI in a way that is consistent with our values and the U.S. Constitution, and that addresses privacy.
- (5) Review IRM 10.5.1.3.2.3, Minimizing Collection, Use, Retention, and Disclosure.

10.5.1.6.22.4
(05-08-2025)
**Openness and Consent
for AI**

- (1) In the context of AI, the IRS privacy principle of openness includes the ability to understand how the AI made the decision. As much as practical, without unduly exposing sensitive information, describe the AI decision-making process in the privacy documentation, such as a PCLIA or AI risk assessment. This documentation informs individuals about the uses to which they consent when they provide data. [Privacy Act sections (e)(2) and (e)(3)]
- (2) The *EO 13960 (external)* AI principle **Transparent** requires agencies to be transparent in showing relevant information about the use of AI. When AI use is appropriately transparent, it protects privacy.
- (3) During the development of AI, consider allowing users to opt out of having their information included in AI, where practical.
- (4) Review IRM 10.5.1.3.2.4, Openness and Consent.

10.5.1.6.22.5
(05-08-2025)
**Strict Confidentiality for
AI**

- (1) Under the IRS privacy principle for strict confidentiality, IRS users, developers, and providers of AI must protect data and share it only with authorized individuals and systems. [Privacy Act section (b); IRC 6103]
- (2) This means that, to mitigate the risks of unauthorized disclosures and data exploitation, you must make sure that the AI use is lawful, secure, and take steps to lessen privacy and confidentiality risks.

- (3) With AI use, make sure the data you share is only accessible by those with a need to know (including other systems). Make sure safeguards are in place to purge data or otherwise prevent re-disclosure after the authorized AI use.
- (4) You are responsible for the information you share when using AI, which includes considering how the AI might use the information later.
- (5) Review IRM 10.5.1.3.2.5, Strict Confidentiality.

10.5.1.6.22.6
(05-08-2025)
Security for AI

- (1) Under the IRS privacy principle for security, AI requires special attention to make sure that developers build it to protect the administrative, technical, and physical access to the system and its data. Use only IRS-approved AI that follow AI risk management, privacy, and security policies. [Privacy Act section (e)(10)]
- (2) AI use cases must follow all relevant IRS privacy and security policies, such as those in this IRM and the IRM 10.8 series.
- (3) The *EO 13960 (external)* principle **Safe, secure, and resilient** requires agencies to ensure the safety, security, and resiliency of AI applications.
- (4) For AI use, take steps to ensure the security of the system and the data it uses. For more information, refer to *National Institute of Standards and Technology (NIST) AI 100-1*, Artificial Intelligence Risk Management Framework (NIST AI 100-1), with further details in IRM 10.8.1, Security Policy, and IRM 10.5.1.8, NIST 800-53 Security and Privacy Controls.
- (5) Review IRM 10.5.1.3.2.6, Security.

10.5.1.6.22.7
(05-08-2025)
Data Quality for AI

- (1) Under the IRS privacy principle for data quality, because many types of AI keep data for future uses, make sure that the data used by AI is accurate, complete, and current. As much as possible, use data collected directly from the individual to whom it relates. [Privacy Act sections (e)(5) and (e)(6)]
- (2) To help ensure data quality, review the results for incorrect conclusions that may impact an individual's rights and civil liberties, whether the result of human inputs or generated from the AI's misunderstanding of the data or directives given to it.
- (3) The *EO 13960 (external)* principle **Accurate, reliable, and effective** instructs agencies to make sure that the application of AI is consistent with the use cases for which that AI was trained, and such use is accurate, reliable, and effective.
- (4) Review IRM 10.5.1.3.2.7, Data Quality.

10.5.1.6.22.8
(05-08-2025)
Verification and Notification for AI

- (1) Under the IRS privacy principle for verification and notification, verify and validate data with AI use as much as possible, including the source of the data. Verification includes leveraging a human review process before taking adverse action based on data used or produced by AI. Where practical, let individuals know about AI use when you collect their data and tell them how to contest inaccurate information. [Privacy Act sections (e)(2), (e)(3), (e)(4), and (e)(6)]

- (2) The *EO 13960 (external)* principle **Regularly monitored** expects agencies to make sure they regularly test AI applications against these principles and stop the use of any AI that does not perform as intended.

- (3) Review IRM 10.5.1.3.2.8, Verification and Notification.

10.5.1.6.22.9
(05-08-2025)

Access, Correction, and Redress for AI

- (1) Under the IRS privacy principle for access, correction, and redress, with AI use, you must be able to give individuals access to and the ability to correct their PII upon request where practical. Programs and processes that use AI must make sure individuals can contest determinations made based on allegedly incomplete, inaccurate, or out-of-date information. [Privacy Act section (d)]

- (2) Where practical, you should have a correction and redress process for individuals impacted by AI-informed decisions or actions based on faulty data. That correction and redress process should include a human.

- (3) Review IRM 10.5.1.3.2.9, Access, Correction, and Redress.

10.5.1.6.22.10
(05-08-2025)

Privacy Awareness and Training for AI

- (1) Under the IRS privacy principle for awareness and training, IRS users, developers, and providers of AI must remain current with IRS privacy and awareness training requirements. For IRS personnel who use AI, make sure they have current guidance and training on how to effectively apply the privacy principles when using AI. As such, you are responsible for protecting the privacy of individuals whose data the AI uses. [Privacy Act section (e)(9)]

- (2) This means the IRS must make sure that AI training follows the privacy principles in its analysis, storage, and use of data. A best practice includes using privacy enhancing technologies and techniques to train AI to follow IRS Privacy Principles. [NIST AI 100-1]

- (3) The EO 13960 principle **Accountable** says that agencies must provide training to all agency personnel responsible for AI use.

- (4) Review IRM 10.5.1.3.2.10, Privacy Awareness and Training.

10.5.1.7
(05-08-2025)

Privacy-Related Programs

- (1) The IRS promotes a robust privacy program leveraging the use of technology and privacy processes. The IRS privacy program improves taxpayer service by protecting the privacy of taxpayers' and employees' data and enhancing their trust. Designing privacy into the IRS modernization initiative (people, systems, processes, and technology) further improves the protection of SBU data (including PII and tax information) throughout the IRS.

- (2) Privacy issues are integral to IRS business. While PGLD owns most privacy-related programs, because of the complexity, scope, and importance of privacy to the IRS mission, some privacy-related programs reside outside of PGLD. For example, PGLD takes part in various privacy-related governance boards managed by other business units.

- (3) This IRM gives links and references to other IRMs and programs that work closely with PPC or have elements of privacy within those programs. IRS personnel must familiarize themselves with and use all links and reference IRMs, as necessary. This includes the privacy-related programs in the following subsections, not all managed by PGLD.

- (4) For more information about PGLD, refer to IRM 1.1.27, Privacy, Governmental Liaison and Disclosure (PGLD), and the *internal PGLD Disclosure and Privacy Knowledge Base*.

10.5.1.7.1
(12-31-2020)
IRS Privacy Council

- (1) Within PGLD's PPC, PPKM oversees and coordinates the IRS Privacy Council.
- (2) The purpose of the IRS Privacy Council is to:
- a. Develop a cohesive privacy vision to implement and oversee IRS-wide privacy and disclosure policies.
 - b. Serve as a high-level strategy and policy development group charged with identifying and effectively addressing significant current and emerging information privacy, disclosure, and related policy issues.
 - c. Centralize the CPO's policy-making role in the development and evaluation of legislative, regulatory, and other policy proposals, which implicate information privacy issues. In so doing, the Council takes a central role in ensuring the IRS is fully compliant with federal laws, regulations, and policies relating to information privacy while enabling continued progress and innovation.
- (3) To carry out these objectives, the IRS Privacy Council members will:
- a. Engage the business units and operating divisions for purposes of multi-level identification of issues appropriate for Council action.
 - b. Partner with cross-functional working groups to identify and work issues appropriate for Council action.
 - c. Generate policy guidance to be issued from the CPO.
 - d. Establish communications and web strategies to ensure successful dissemination of guidance and more tools for ongoing IRS-wide education and assistance.
 - e. Conduct periodic reviews of established policy guidance to ensure sufficiency and consistency.
 - f. Partner with Office of Chief Counsel for consultative purposes, and to identify and develop needed legislative and regulatory proposals.
 - g. Review and comment on circulated draft legislation, executive orders, Office of Management and Budget memoranda, executive agency white papers, and other inter-governmental documents.
 - h. Provide subject matter expertise on broad-scope IRS-wide initiatives.
 - i. Partner with program offices to ensure inclusion of information privacy, records, and disclosure policies are appropriately included in training modules. [Accountability]
- (4) The IRS privacy community takes part in the Federal Privacy Council (FPC) to identify federal agency best practices, build and strengthen collaboration with other agencies, and conduct outreach as proper. Review Exhibit 10.5.1-2, References, for the link to the FPC website and resources.
- (5) For more information, email **Privacy* or refer to the *internal IRS Privacy Council site*.

10.5.1.7.2
(05-08-2025)
Privacy and Civil Liberties Impact Assessment (PCLIA)

- (1) The Privacy Review team in PCA, within PGLD's PPC, supports the IRS in recognizing the importance of protecting the privacy of taxpayers and employees, balancing the need for information collection with the privacy risks. The vehicle for addressing privacy issues in a system is the PCLIA. [E-Government Act, OMB A-130, RA-08]

- (2) When the IRS procures, uses, or develops IT to process PII, the IRS must consider the privacy protections with a PCLIA. The IRS requires PCLIA's for pilot projects, research, experimentation, the use of innovative technologies, technical demonstrations, prototypes, and proof of concepts, and the like. [E-Government Act, RA-08]
- (3) For more information about the PCLIA process, refer to IRM 10.5.2.2 , Privacy and Civil Liberties Impact Assessment (PCLIA), or the *internal PCLIA site*. For questions, email **Privacy Review*.

10.5.1.7.3
(05-08-2025)
**Business PII Risk
Assessment (BPRA)**

- (1) The Business PII Risk Assessment (BPRA) program in PGLD's PPC assesses privacy risks in IRS processes. The BPRA addresses the impact of privacy risks in the same way an IT security risk assessment addresses the impact of security risks to the IRS. [OMB A-130]
- (2) For more information, refer to IRM 10.5.2.4 , Business PII Risk Assessment (BPRA), and the *internal BPRA site*.

10.5.1.7.4
(05-08-2025)
**Privacy Control
Assessment Teams
(PCAT)**

- (1) The Privacy Control Assessment Teams (PCAT) in PCA, within PGLD's PPC, conduct assessments to determine the extent to which the privacy controls from IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls, are implemented correctly, operating as intended, and producing the desired outcome. The PCAT process assigns risks identified during the assessments to the proper functional area for resolution and reporting.
- (2) For more information about the PCAT process, refer to the *internal Privacy Control Assessment Team site* or email **PGLD PCAT*.

10.5.1.7.5
(05-08-2025)
Privacy Reporting

- (1) Privacy reporting comes through several offices within PGLD. [PM-27]
- (2) Refer to the *internal PGLD - All Internal and External Reports site*, IRM 10.5.1.8.10.24, PM-27 Program Management -- Privacy Reporting [P] {Org}, IRM 10.5.6.9, Privacy Act Reports, and IRM 10.5.2.3, Reporting.

10.5.1.7.6
(05-08-2025)
UNAX Program

- (1) Information Protection Projects (IPP), under PGLD's Identity and Records Protection (IRP), manages the UNAX program to implement the requirements of the Taxpayer Browsing Protection Act.
- (2) The UNAX program provides awareness to make sure you do not compromise public confidence in our protection of tax account information.
- (3) For more information, refer to IRM 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements.
- (4) Refer to the *internal UNAX site*.

10.5.1.7.7
(05-08-2025)
Mandatory Briefings

- (1) Mandatory briefings deliver required IRS-wide training, including the Privacy Information Protection and Disclosure, Records Management, CUI, and UNAX briefings managed by the PGLD offices of PPKM, IRP, and IPP, respectively. [AT-03]
- (2) For more information about mandatory briefings, refer to the *internal Mandatory Briefings site*.

10.5.1.7.8
(05-08-2025)

Records and Information Management (RIM)

- (1) Records and Information Management (RIM) Office within PGLD's IRP supports the IRS mission and programs by promoting current information, guidance, and awareness of the importance of managing records throughout the IRS. The RIM program addresses the requirements for recordkeeping, protection, review, storage, and disposal.
- (2) The public expects that IRS records are available where and when they are needed, to whom they are needed, for only as long as they are needed, to conduct business, adequately document IRS activities, and protect the interests of the federal government and taxpayers. The Federal Records Act requires the IRS to efficiently manage all IRS records until final disposition.
- (3) For more information about records, refer to the IRM 1.15 series, Records and Information Management, or the records management pages on the *internal PGLD Disclosure and Privacy Knowledge Base*.

10.5.1.7.9
(05-08-2025)

Disclosure

- (1) Disclosure, within PGLD's Governmental Liaison, Disclosure and Safeguards (GLDS), manages FOIA and IRC 6103 policy to make sure the right information is released to the right individuals at the right time. They deliver timely public access to IRS records under disclosure laws. They make sure IRS employees understand disclosure rules and know how to protect federal tax information, taxpayer confidentiality, and privacy.
- (2) Under IRC 6103, tax returns and return information are confidential information that we must not disclose except as allowed by the IRC.

Note: IRC 7213 and IRC 7431 include civil and criminal penalties for willful or negligent disclosure of returns or return information.

- (3) The IRM 11.3 series, Disclosure of Official Information, has policy on whether we may disclose tax returns and other information contained in IRS files. Make no disclosure unless IRC 6103 authorizes disclosure and not before meeting requirements in IRC 6103 and the IRM 11.3 series.
- (4) For more information, refer to the disclosure pages on the *internal PGLD Disclosure and Privacy Knowledge Base*.
- (5) For external FOIA requests, refer to *FOIA (external)*.

10.5.1.7.10
(05-08-2025)

Digital Identity Risk Assessment (DIRA)

- (1) Digital Identity Risk Assessment (DIRA) is a joint effort between IT Cybersecurity and Online Services to form a framework for establishing authentication risk consistently across online web-based electronic transactions. The DIRA process applies to online web-based transactions. [NIST SP 800-63]
- (2) To ensure privacy and security, agencies must authenticate users of their web-based or online transactions before allowing access to information entrusted to them. The DIRA process evaluates the risk of a transaction to decide the applicable assurance level on three parts, referred to as *Identity Assurance Level (IAL)*, *Authenticator Assurance Level (AAL)*, and *Federation Assurance Level (FAL)*.
- (3) For more information, refer to the *internal Digital Identity Risk Assessment (DIRA) site*. For information about risk assessments of online services, contact **IT Cyber CPO DIRA*.

- 10.5.1.7.11
(05-08-2025)
One Solution Delivery Life Cycle (OneSDLC)
- (1) The IRS IT OneSDLC process is how the IRS manages project activities.
 - a. OneSLDC provides the direction, processes, tools, and assets necessary to carry out business change in a consistent and repeatable manner as they implement the EA.
 - b. OneSDLC replaced the ELC. OneSDLC has 3 stages: Allocation, Readiness, and Execution.
 - (2) For more information about OneSDLC, refer to IRM 2.31.1, One Solution Delivery Life Cycle Guidance, or the *OneSDLC site*.
- 10.5.1.7.12
(12-31-2020)
Governmental Liaison (GL)
- (1) Governmental Liaison (GL) facilitates, develops, and maintains relationships with federal, state, and local governmental agencies and IRS operating and functional divisions on strategic IRS programs. Contact GL before contacting any governmental agency about initiatives or data exchanges.
 - (2) GL maintains the IRS Agreement Database (IAD), which includes formal agreements that GL established with U.S. federal, state and local governmental agencies and IRS business units to exchange data, and tax and non-tax information that require PGLD oversight for privacy, disclosure, and safeguarding. Internet service agreements, LB&I treaty and Foreign Account Tax Compliance Act agreements, agreements with 6103(k)(6) disclosures and IRC 6103(c) consent-based disclosures with non-government agencies are excluded.
 - (3) For more information about GL, refer to IRM 11.4.1, Governmental Liaison Operations.
 - (4) For more information about GL's programs, refer to the *internal GL site*.
- 10.5.1.7.13
(07-08-2021)
Data Services
- (1) Data Services provides support to GL and Disclosure programs through a variety of information technology initiatives, including:
 - Managing computer matching agreements (CMAs).
 - Managing the Governmental Liaison Data Exchange Program (GLDEP).
 - (2) For more information about Data Services, refer to IRM 11.4.2, Data Exchange Program, and IRM 11.3.39, Computer Matching and Privacy Protection Act.
- 10.5.1.7.14
(05-08-2025)
Identity Assurance (IA)
- (1) Identity Assurance (IA) provides oversight and strategic direction for authentication, authorization, and access processes of taxpayer information. IA also delivers externally facing IRS services across all channels while protecting taxpayer data from fraudsters and identity thieves.
 - (2) For more information about IA, refer to the IRM 10.10 series, Identity Assurance, and the identity assurance pages on the *internal PGLD Disclosure and Privacy Knowledge Base*.
- 10.5.1.7.14.1
(05-08-2025)
Electronic Signature (e-Signature) Program
- (1) Managed by PGLD's IA, the IRS e-signature principles and federally mandated authentication controls describe how the IRS protects an individual's identity and assures that only authorized signers are completing the transaction.
 - (2) For more information, refer to IRM 10.10.1 , IRS Electronic Signature (e-Signature) Program, and the *internal e-Signature site*. For questions, email the **PGLD IA eSignature mailbox*.

10.5.1.7.14.2
(05-08-2025)

**Non-Digital
Authentication Risk
Assessment (NDARA)**

- (1) The PGLD IA IRM 10.10.2, Authentication Risk Assessments in Non-Digital Channels, details this policy as part of their omni channel approach to authentication and authorization for all interactions.
- (2) For electronic interactions, this policy defers to the DIRA process for electronic interactions. Review IRM 10.5.1.7.10, Digital Identity Risk Assessment (DIRA). For all other interactions, this policy applies to assessing the risk in the authentication process of telephone, in-person, and correspondence exchanges of sensitive information with individuals in authenticated customer contact channels.
- (3) For more information, refer to the *internal NDARA site*.
- (4) For questions, email **PGLD IA Omni-Innovations*.

10.5.1.7.15
(05-08-2025)

IT Security

- (1) IT Security Policy, within Cybersecurity, supports IT security policy and implementation.
- (2) IT security and privacy issues go together. IT security policy describes how to protect IT environments, while privacy policy describes how to protect individuals' information in those IT environments. IT focuses on protecting the systems, the network, and the applications that house the data. Privacy focuses on protecting the individual represented by the data.
- (3) For more information about IT security policy and references, refer to the IRM 10.8 series, Information Technology (IT) Security.
- (4) For more information about the Cybersecurity program, refer to the *internal Cybersecurity site*.

10.5.1.7.16
(09-15-2023)

**Incident Management
(IM)**

- (1) Within PGLD's PPC, the IM program is dedicated to helping taxpayers and personnel potentially affected by IRS data breaches by working quickly and thoroughly to investigate data breaches to decrease the possibility that information will be compromised and used to perpetrate identity theft or other forms of harm.

Note: IM is not responsible for any disciplinary actions that can result for an employee's or manager's failure to protect IT equipment or information, or for an employee's or manager's failure to protect employee data or PII.

- (2) The IM program manages reports of IRS losses, thefts, and inadvertent unauthorized disclosure of SBU data (including PII and tax information).
- (3) Immediately upon discovery of an inadvertent unauthorized disclosure of sensitive information, or the loss or theft of an IT asset or hardcopy record or document that includes sensitive information, personnel must report an incident and data breach to the manager and the proper organizations based on what was lost or disclosed.
- (4) Anyone discovering a data breach must report the data breach to the proper organizations.
- (5) For more information about how to report an incident and data breach, refer to IRM 10.5.4.3, Reporting Losses, Thefts and Disclosures, or the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.

10.5.1.7.17
(05-08-2025)
Pseudonym

- (1) The IM Employee Protection group, within PGLD's PPC IM, manages the IRS pseudonym program.
- (2) Under certain conditions (including protection of personal safety, adequate justification, and pre-approval), this program allows for the use of pseudonyms by IRS employees. The Employee Protection group helps employees protect the privacy of these pseudonyms.
- (3) Refer to IRM 10.5.7, Use of Pseudonyms by IRS Employees.

10.5.1.7.18
(05-08-2025)
Safeguards

- (1) The Safeguards program makes sure that federal, state, and local agencies receiving federal tax information protect it as if the information remained in IRS's hands, using Pub 1075, Tax Information Security Guidelines for Federal, State and Local Agencies.
- (2) For more information about Safeguards, refer to IRM 11.3.36 , Safeguard Review Program, and the *internal Safeguards site*.

10.5.1.7.19
(05-08-2025)
Social Security Number Elimination and Reduction (SSN ER)

- (1) Information Protection Projects (IPP), under PGLD's IRP, manages the Social Security Number Elimination and Reduction (SSN ER) program.
- (2) This program's goal is to implement regulatory requirements to eliminate or reduce the collection and use of SSNs in programs, processes, and forms. [Pub.L. 115-59, OMB A-130, PT-07(01)]
- (3) For more information, refer to the *internal SSN ER site* or email **PGLD SSN Reduction*.

10.5.1.7.19.1
(03-23-2018)
Acceptable Use of SSNs

- (1) Use of SSNs is acceptable when any of these options mandates such use:
 - Law or statute.
 - Executive orders.
 - Federal regulations.
 - Business need (such as the inability to alter systems, processes, or forms due to costs or unacceptable level of risk).

10.5.1.7.19.2
(05-08-2025)
Creating and Revising IRS Products

- (1) You must use Form 14132, Social Security Number Retention Justification for Forms, Letters, Notices, and Systems, for new and revised products with SSNs during the Publishing Service Request (PSR) and Office of Taxpayer Correspondence (OTC) Request for Services processes. The completion of this form will make sure requesters evaluate the need for using an SSN while also allowing PGLD to effectively track the use of SSNs within correspondence process. Procedures include creating or revising:
 - a. Non-tax forms (Media and Publications).
 - b. IRS correspondence (OTC).
 - c. Tax forms (Tax Forms and Publications).
- (2) **Non-tax forms (Media and Publications):** Media and Publications can not process Request for Services for new forms with SSNs, or revised forms with a change to a TIN field, until OTC receives verification of a signed Form 14132. This table outlines the process:

Who	Process for non-tax forms
Requester	Sends a completed Form 14132 to PGLD at <i>*PGLD SSN Reduction</i> before sending a PSR for products with SSNs or TINs.
PGLD	Monitors the organizational mailbox and signs completed Form 14132 within five business days of receipt.
PGLD	Keeps a list with new and revised inventory.
PGLD	Uploads, stores, and keeps signed forms on the e-Trak system and runs periodic reports to track mitigation.
PGLD	Works with business units to resolve concerns as needed.
PGLD	Conducts reviews and data calls every three years to update Form 14132, if applicable.

- (3) **IRS correspondence (OTC):** OTC can not process Request for Services for new forms with SSNs, or revised forms with a change to a TIN field, until OTC receives verification of a signed Form 14132. This table outlines the process:

Who	Process for IRS correspondence
Requester	Sends a completed Form 14132 to PGLD at <i>*PGLD SSN Reduction</i> before sending an OTC Request for Services for correspondence with SSNs or TINs.
PGLD	Monitors the organizational mailbox and signs completed Form 14132 within five business days of receipt.
PGLD	Keeps a list with new and revised inventory.
PGLD	Uploads, stores, and keeps signed forms on the e-Trak system and runs periodic reports to track mitigation.
PGLD	Works with business units to resolve concerns as needed.
PGLD	Conducts reviews and data calls every three years to update Form 14132, if applicable.

- (4) **Tax forms (Tax Forms and Publications):** This table outlines the process:

Who	Process for tax forms
Tax law specialist (TLS) TLS reviewer Section chief	Checks with their respective branch or division manager before issuing a PSR for new or revised tax forms when they contain fields for SSNs or TINs of an individual (such as an ATIN or ITIN) other than the SSN or TIN of the filer.
Senior tech advisor (STA) Lead TLS	Reviews and approves the new or revised tax form.

Who	Process for tax forms
STA or TLS	<p>If the approved revision of a tax form results in the removal of an SSN entry space or approved new form includes an SSN entry space, STA or TLS will:</p> <ul style="list-style-type: none"> Alert PGLD by email at pgld.ssn.reduction@irs.gov and provide the form number and BOD contact(s). Inform BOD they must provide a legal justification for requesting the SSN or TIN to Tax Forms and Publications. Inform BOD they must provide a legal justification for requesting an SSN or TIN to PGLD by sending Form 14132.
PGLD	Monitors the organizational mailbox and signs completed Form 14132 within five business days of receipt.
PGLD	Keeps a list with new and revised inventory.
PGLD	Uploads, stores, and keeps signed forms on the e-Trak system and runs periodic reports to track mitigation.
PGLD	Works with business units to resolve concerns as needed.
PGLD	Conducts reviews and data calls every three years to update Form 14132, if applicable.

10.5.1.7.19.3
(05-08-2025)
**SSN Necessary-Use
Criteria**

- (1) SSN ER compliance requires owners of forms, notices, letters, and systems to apply the following SSN necessary-use criteria to verify whether SSN use is justifiable and necessary.
- (2) **Apply the SSN Necessary-Use Criteria:** Based on the definition of the necessary or acceptable use of SSNs.
- (3) Give an accurate and complete citation of what authority (legislative mandate, regulation, or executive order) justifies SSN usage.
- (4) Consider how we use the SSN throughout the information lifecycle (reviewing all forms, notices, letters, and systems), and consider the following about SSN data:
 - Acquisition or collection
 - Conversion or use and display
 - Migration or transmission
 - Storage
 - Deletion or disposal
- (5) Verify whether the SSN is a critical part to the business process, which we cannot perform or achieve without the use of the SSN. The owner must describe in detail those existing operational dependencies. Use Form 14132.
- (6) **Identify SSN Elimination and Reduction Solutions:** After identifying potential areas to reduce or eliminate SSN use, collaborate with business unit stakeholders to explore and identify workable short- and long-term mitigation solutions, and send a written mitigation plan to IPP by email to **PGLD SSN Reduction*.
- (7) **Develop a Mitigation Strategy for Existing Inventories:** Whether SSN use is verified to be necessary or unnecessary, develop and provide to IPP a mitigation strategy for existing forms, notices, and letters inventories on Form 14132.

- (8) **When Creating New Forms, Notices, Letters, and Systems:** Business and system owners must practice due diligence when creating new forms, notices, letters, and systems to make sure they apply the necessary-use criteria. Use this table:

For New...	The Process Is...
Forms	Taxpayer Services (TS) Media and Publications will ask form owners to consider the necessary use of SSNs on newly created forms. You must provide justification for all forms requiring an SSN. The justification will become part of the form history folder. (For required Privacy Act Notification information, refer to IRM 10.5.6.4, Privacy Notices.)
Notices or Letters	The Office of Taxpayer Correspondence will ask owners to consider use of SSNs on all newly created notices or letters. These questions and answers will become part of the interview file and kept for documentation purposes.
Systems	Owners must complete a Privacy and Civil Liberties Impact Assessment (PCLIA) for any system that will contain any personally identifiable information, including SSNs. The purpose of a PCLIA is to show that program or project managers and system owners and developers have consciously incorporated privacy and civil liberties protections throughout the entire lifecycle of a system. The Privacy Impact Assessment Management System will keep the justification for SSN usage. [RA-08]

- (9) **Manage Inventory:** PGLD will use completed Form 14132 to manage the SSN ER Program and report progress to Treasury and IRS executive leadership.
- (10) **Reassess Periodically:** Once every three years, business or systems owners must reassess any forms, notices, letters, or systems to verify whether conditions have changed that allow for the elimination or masking the SSN on their products. Business or system owners must inform the SSN ER Program of updated statuses on each product.

10.5.1.7.20
(12-31-2020)
**SBU Data Use for
Non-Production
Environments**

- (1) Within PGLD's PPC, PCA manages the SBU Data Use process for non-production environments.
- (2) The SBU Data Use for non-production environments process helps information owners (IOs) and authorizing officials (AOs) know when we are using SBU data (including PII or tax information) in other non-production environments, when proper. This process helps IOs and AOs, tasked with accepting risk for the IRS, to know and understand the movement of the SBU data outside the production environment and to ensure its protection.
- (3) Refer to IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments, and the *internal SBU Data Use Process site*.

10.5.1.7.21
(05-08-2025)
**Quick Response (QR)
Codes**

- (1) The Office of Taxpayer Correspondence in Media and Publishing manages the Quick Response (QR) codes for the IRS to provide taxpayers with targeted, prompt guidance and outreach.
- (2) Using IRS-created QR codes allows the IRS to minimize data collection (to collect only necessary data), to protect privacy and civil rights, to reduce costs, and to make sure that the experience instills trust and consistency.

- (3) Refer to IRM 1.17.7.4.8, QR Response (QR) Codes.

10.5.1.8
(05-08-2025)
**NIST SP 800-53 Security
and Privacy Controls**

- (1) These privacy and security controls are the technical controls that address federal IT systems. These privacy requirements and technical controls build on the existing IRS Privacy Principles and supplement the full range of existing security controls in IRM 10.8.1, Security Policy. This subsection addresses all the controls relevant to privacy and applies to security and privacy authorization to operate.
- (2) This subsection is for technical management officials developing and supporting IT systems, including management, senior management and executives, system owners, system developers, and authorizing officials.
- (3) NIST SP 800-53 has these definitions: [NIST SP 800-53]
 - *Controls* can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. Controls are selected and implemented by the organization to satisfy the system requirements. Controls can include administrative, technical, and physical aspects.
 - For federal information security and privacy policies, the term *requirement* is generally used to refer to information security and privacy obligations imposed on organizations.
 - The term *requirement* can also be used in a broader sense to refer to an expression of stakeholder protection needs for a system or organization. Stakeholder protection needs and the corresponding security and privacy requirements may be derived from many sources (such as laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments).
 - The term *processing* collectively refers to “the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal” of PII.
- (4) Each control family falls under its own subsection of IRM 10.5.1.8, starting with the -01 Policy and Procedures control for that family. Under the family subsection, its subsections list the other controls in that family and their enhancements. For example, the Awareness and Training (AT) family starts with the AT-01 control in the subsection IRM 10.5.1.8.2, AT-01 Awareness and Training — Policy and Procedures [J] {Org}. Within the AT family, it has four applicable controls or enhancements, shown as its 4 subsections:
 - IRM 10.5.1.8.2.1, AT-02 Awareness and Training — Literacy Training and Awareness [J] {Org}
 - IRM 10.5.1.8.2.2, AT-03 Awareness and Training — Role-Based Training [J] {Org}
 - IRM 10.5.1.8.2.3, AT-03(5) Awareness and Training — Role-Based Training - Processing Personally Identifiable Information [P] {Org}
 - IRM 10.5.1.8.2.4, AT-04 Awareness and Training — Training Records [J] {Org}
- (5) This subsection’s naming structure follows the pattern shown in this table, with **AC-03(14) Access Control — Access Enforcement - Individual Access [P] {Org}** as an example:

Name	Explanation
AC-03	The 2-letter control abbreviation NIST uses for the control family with a dash and the control number (uses leading 0 if single digit).
(14)	<i>This part is only for the control enhancements (CEs).</i> The CE number is in parentheses and merged with the control enhancement number (IRM 10.8.1, Security Policy, uses this convention).
Access Control	Control family name.
Access Enforcement	Control name.
Individual Access	Control enhancement name, if applicable.
[P] for privacy	If a control is privacy-owned [P], the language of the control is in this IRM.
[J] for joint security and privacy	If security and privacy [J] jointly own a control, the language of the control is in IRM 10.8.1.
[S] for security	The security-owned [S] controls are in IRM 10.8.1.
{Org}	Organizational common control (OCC).
{Sys}	System control.
{Hybrid}	Hybrid OCC and system control.
[L, M, H]	Low, moderate, high. This IRM does not list these because all joint and privacy controls apply to all low, moderate, and high systems. You will see these in IRM 10.8.1. Note: Privacy is about the data, not the system.

(6) This table explains how this IRM shows the control information:

If the control is ...	Then the IRM subsection ...
Joint	First paragraph references the IRM 10.8.1 subsection.
Privacy	First paragraph(s) repeat the NIST control language (ending with the attribution [NIST SP 800-53]), with <i>any IRS organization-defined parameters italicized</i> .
Differs from the NIST baseline	Note to first paragraph(s) explains how it differs or how the IRS will assess it differently.
Not a -01 Policy and Procedures control	Next paragraph after the control language summarizes the IRS policy requirement that links to the IRS Privacy Principles.
Is a -01 Policy and Procedures control	Skips summary of IRS policy requirement.

If the control is ...	Then the IRM subsection ...
Any control listed	Next paragraph after the summary gives implementation guidance , which summarizes how the IRS implements that control to address the requirement. The organization may use this guidance as the basis for implementation statements in assessments of organizational controls. Note: Every information collection is unique; when questions arise needing consultation, contact <i>*Privacy</i> .
Any control listed	Next paragraph after implementation guidance lists references to policies within this IRM 10.5.1 on the control. (Subsections referenced include all its subsections, with specific subsections sometimes listed for emphasis.)
Any control listed	Next paragraph after IRM 10.5.1 references lists references to other PGLD and IRS policies that supplement the control. (Subsections referenced include all its subsections, with specific subsections sometimes listed for emphasis.)

- (7) For more specific implementation guidance, refer to the Privacy Controls Checklist on the *internal Privacy Controls site*.

10.5.1.8.1

(05-08-2025)

**AC-01 Access Control —
Policy and Procedures
[J] {Org}**

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about access control. For the full text of the control, refer to IRM 10.8.1.4.1, AC-01 Access Control Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
- Control access to those authenticated and authorized individuals with a need to know.
 - Allow access by individuals to their own information as allowed by law.
- (3) In this IRM, follow the policies on the access control policy and procedures control, including:

IRM	Title
IRM 10.5.1.1.1	Purpose of the Program
IRM 10.5.1.1.2	Audience
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.5.1	Clean Desk Policy
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data
IRM 10.5.1.6.2	Encryption
IRM 10.5.1.6.3	Computers and Mobile Computing Devices

IRM	Title
IRM 10.5.1.6.6	Storage
IRM 10.5.1.6.8.2	Emails to Other External Stakeholders
IRM 10.5.1.6.10	Disposition and Destruction
IRM 10.5.1.6.15	Contracts
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices
IRM 10.5.1.6.18	Data on Collaborative Technology and Systems

- (4) Follow the other PGLD and IRS policies that supplement the access control policy and procedures control, including:

IRM	Title
IRM 10.5.2.1	Program Scope and Objectives
IRM 10.5.2.1.1	Background
IRM 10.5.2.2.5.2	Privacy Compliance in Collaborative Environments (formerly Shared Storage PIAs)
IRM 10.5.6.3.5	Content of a SORN
IRM 10.5.5.1	Program Scope and Objectives
IRM 10.5.5.2	IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program
IRM 10.5.5.3	Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
IRM 11.3.22.2.1	Access by IRS Employees
IRM 1.2.1.2.1	Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights
IRM 1.2.1.17.2	Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safeguarding Confidential Tax Information

10.5.1.8.1.1
(05-08-2025)
AC-03(14) Access Control — Access Enforcement - Individual Access [P] {Org}

- (1) The IRS must provide *information on IRS.gov/privacy* to enable individuals to have access to the elements of their personally identifiable information *that the IRS collects, as governed by the applicable laws and regulations*. [NIST SP 800-53] [OMB M-21-04]
- (2) The IRS requires giving individuals access to their IRS information, as allowed.
- (3) **Implementation guidance:** The IRS implements this control by requiring publishing of Privacy Act requests information on IRS.gov/privacy, publishing SORNs and PCLIAAs, and handling requests for information under the Privacy Act, IRC, and FOIA. Instructions in IRM 10.5.6.6 , Privacy Act Requests for Non-Tax Records, give employees procedures for making requests to access this information.

- (4) To meet this control, you must follow the policies in this IRM on the individual access control, including:

IRM	Title
IRM 10.5.1.3.2.9	Access, Correction, and Redress
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices

- (5) Follow the other PGLD and IRS policies that supplement the individual access control, including:

IRM	Title
IRM 10.5.2.2.4.5	PCLIAs or IRS.gov
IRM 10.5.6.3	Privacy Act SORNs
IRM 10.5.6.6	Privacy Act Requests for Non-Tax Records
IRM 11.3.13.3.11	Routine Established Agency Procedures

10.5.1.8.2
(05-08-2025)
AT-01 Awareness and Training — Policy and Procedures [J] {Org}

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about awareness and training control. For the full text of the control, refer to IRM 10.8.1.4.2, AT-01 Awareness and Training Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
- Remain aware of and trained on the proper treatment of SBU data, including PII and tax information based on their roles.
 - Track such training records.
- (3) In this IRM, follow the PGLD policies on the awareness and training policy and procedures control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data
IRM 10.5.1.6.15	Contracts
IRM 10.5.1.7.1	IRS Privacy Council
IRM 10.5.1.7.7	Mandatory Briefings

- (4) Follow the other PGLD and IRS policies that supplement the awareness and training policy and procedures control, including:

IRM	Title
IRM 10.5.2.1	Program Scope and Objectives
IRM 10.5.2.2.3	PCLIA Roles and Responsibilities
IRM 10.5.4.1	Program Scope and Objectives
IRM 10.5.4.1.3	Responsibilities
IRM 10.5.4.2	Awareness Training and Education
IRM 10.5.5.3	Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
IRM 10.5.6.2.8	Privacy Act Training
IRM 11.3.1.1.3	Roles and Responsibilities
IRM 1.15.1.3	Oversight Responsibilities
IRM 1.1.27.1.4	Roles and Responsibilities

- 10.5.1.8.2.1
(05-08-2025)
AT-02 Awareness and Training — Literacy Training and Awareness [J] {Org}
- (1) This is a joint security and privacy control about literacy training and awareness. For the full text of the control, refer to IRM 10.8.1.4.2.1, AT-02 Literacy Training and Awareness (InTC).
 - (2) The IRS requires keeping personnel current on privacy training and awareness.
 - (3) **Implementation guidance:** The IRS implements this control by requiring annual mandatory briefings on security and privacy. PGLD contributes to the content of the mandatory briefings, incorporating lessons learned or issues of concern. PGLD employs awareness techniques such as all-employee communications, awareness events, and ad-hoc sessions.
 - (4) To meet this control, you must follow the policies in this IRM on the literacy training and awareness control, listed in the AT-01 references, IRM 10.5.1.8.2.
 - (5) Follow the other PGLD and IRS policies that supplement the literacy training and awareness control, listed in the AT-01 references, IRM 10.5.1.8.2

- 10.5.1.8.2.2
(05-08-2025)
AT-03 Awareness and Training — Role-Based Training [J] {Org}
- (1) This is a joint security and privacy control about role-based training. For the full text of the control, refer to IRM 10.8.1.4.2.2, AT-03 Role-Based Training.
 - (2) The IRS requires keeping personnel current on privacy training and awareness.
 - (3) **Implementation guidance:** The IRS implements this control by requiring role-based privacy training for roles with specialized privacy responsibilities.
 - (4) To meet this control, you must follow the policies in this IRM on the role-based training control, listed in the AT-01 references, IRM 10.5.1.8.2.
 - (5) Follow the other PGLD and IRS policies that supplement the role-based training control, listed in the AT-01 references, IRM 10.5.1.8.2

10.5.1.8.2.3
(05-08-2025)

AT-03(5) Awareness and Training — Role-Based Training - Processing Personally Identifiable Information [P] {Org}

- (1) Provide *all personnel with access to PII* with initial and *annual* training in the employment and operation of personally identifiable information processing and transparency controls. [NIST SP 800-53]
- (2) The IRS requires training all personnel who process PII on how to protect privacy before allowing access to PII.
- (3) **Implementation guidance:** The IRS implements this control by requiring initial and annual mandatory briefings on privacy for all personnel who access PII.
- (4) To meet this control, you must follow the policies in this IRM on the processing personally identifiable information control, listed in the AT-01 references, IRM 10.5.1.8.2.
- (5) Follow the other PGLD and IRS policies that supplement the processing personally identifiable information control, listed in the AT-01 references, IRM 10.5.1.8.2

10.5.1.8.2.4
(05-08-2025)

AT-04 Awareness and Training — Training Records [J] {Org}

- (1) This is a joint security and privacy control about training records. For the full text of the control, refer to IRM 10.8.1.4.2.3, AT-04 Training Records.
- (2) The IRS requires tracking the training records to make sure that all personnel are current on privacy training and awareness. [Privacy Awareness and Training]
- (3) **Implementation guidance:** The IRS implements this control by keeping and reviewing records that personnel have taken the annual mandatory briefings on security and privacy.
- (4) To meet this control, you must follow the policies in this IRM on the training records control, listed in the AT-01 references, IRM 10.5.1.8.2.
- (5) Follow the other PGLD and IRS policies that supplement the training records control, listed in the AT-01 references, IRM 10.5.1.8.2.

10.5.1.8.3
(05-08-2025)

AU-01 Audit and Accountability — Policy and Procedures [J] {Org}

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the audit and accountability control. For the full text of the control, refer to IRM 10.8.1.4.3, AU-01 Audit and Accountability Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Limit SBU data (including PII and FTI) in audit logs to only that needed for its intended use.
 - b. Grant access only on a need-to-know basis.
 - c. Document the justification for information collected and shared.
 - d. Follow records management requirements for such data.
- (3) In this IRM, follow the PGLD policies on the audit and accountability policy and procedures control, including:

IRM	Title
IRM 10.5.1.2.8	Need to Know
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.15	Contracts
IRM 10.5.1.6.14.3	Monitoring Individuals
IRM 10.5.1.6.18.4	Cloud Computing

- (4) Follow the other PGLD and IRS policies that supplement the audit and accountability policy and procedures control, including:

IRM or Publication	Title
IRM 10.5.5.1.1	Background
IRM 10.5.5.3	Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.3.1
(05-08-2025)
AU-02 Audit and Accountability — Event Logging [J] {Org}

- (1) This is a joint security and privacy control about event logging. For the full text of the control, refer to IRM 10.8.1.4.3.1, AU-02 Event Logging.
- (2) The IRS requires logging events (such as audit logs, audit trails, or event logs) to make sure only those with a need to know access and share SBU data.
- (3) **Implementation guidance:** The IRS implements this control by requiring systems limit the SBU data (including PII and FTI) in audit logs to only that needed for its intended use, grant access only on a need-to-know basis and document the justification for information collected and shared.
- (4) To meet this control, you must follow the policies in this IRM on the event logging control, listed in the AU-01 references, IRM 10.5.1.8.3.
- (5) Follow the other PGLD and IRS policies that supplement the event logging control, listed in the AU-01 references, IRM 10.5.1.8.3.

10.5.1.8.3.2
(05-08-2025)
AU-03(3) Audit and Accountability — Content of Audit Records - Limit Personally Identifiable Information Elements [P] {Sys}

- (1) Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: *Minimum necessary PII identified in the PCLIA*. [NIST SP 800-53]
- (2) The IRS requires limiting PII in audit records when such information is not needed for operational purposes. This helps reduce the level of privacy risk created by a system. [Minimizing Collection, Use, Retention, and Disclosure; Strict Confidentiality]
- (3) **Implementation guidance:** The IRS implements this control by requiring systems limit PII in audit records to the minimum necessary.

- (4) To meet this control, you must follow the policies in this IRM on the limit personally identifiable information elements control, including:

IRM	Title
IRM 10.5.1.2.8	Need To Know
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.14.3	Monitoring Individuals

- (5) Follow the other PGLD and IRS policies that supplement the limit personally identifiable information elements control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.3.3
(05-08-2025)
AU-11 Audit and Accountability — Audit Record Retention [J] {Org}

- (1) This is a joint security and privacy control about audit record retention. For the full text of the control, refer to IRM 10.8.1.4.3.10, AU-11 Audit Record Retention.
- (2) The IRS requires keeping audit records on FOIA requests, subpoenas, and law enforcement actions for the proper period to maintain transparency.
- (3) **Implementation guidance:** The IRS implements this control by following IRS records managements requirements.
- (4) To meet this control, you must follow the policies in this IRM on the audit record retention control, including:

IRM	Title
IRM 10.5.1.3.2.3	Minimizing Collection, Use, Retention, and Disclosure
IRM 10.5.1.4.4	Systems Owners
IRM 10.5.1.7.8	Records and Information Management (RIM)

- (5) Follow the other PGLD and IRS policies that supplement the audit record retention control, including:

IRM or Publication	Title
IRM 1.15.6.4	Electronic Records
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.4
(05-08-2025)

**CA-01 Assessment
Authorization and
Monitoring — Policy and
Procedures [J] {Org}**

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the assessment authorization and monitoring policy and procedures control. For the full text of the control, refer to IRM 10.8.1.4.4, CA-01 Assessment Authorization and Monitoring Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Assess security and privacy controls.
 - b. Monitor and address privacy risks found.
 - c. Address privacy requirements before authorization to operate.
 - d. Maintain ongoing awareness of developing vulnerabilities.
- (3) In this IRM, follow the PGLD policies on the assessment authorization and monitoring policy and procedures control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.3.1	Privacy Controls
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.18.4	Cloud Computing
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.3	Business PII Risk Assessment (BPRA)
IRM 10.5.1.7.10	Digital Identity Risk Assessment (DIRA)
IRM 10.5.1.7.14.2	Non-Digital Authentication Risk Assessment (NDARA)

- (4) Follow the other PGLD and IRS policies that supplement the assessment authorization and monitoring policy and procedures control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.2.4	Business PII Risk Assessment (BPRA)
IRM 10.5.6.2.9	OMB Privacy Act Guidance
IRM 10.5.6-1	Agency Review Requirements
Pub 5499	IRS Privacy Program Plan
n/a	<i>internal Privacy Control Assessment Team site</i>

10.5.1.8.4.1
(05-08-2025)
**CA-02 Assessment
Authorization and
Monitoring — Control
Assessments [J] {Sys}**

- (1) This is a joint security and privacy control about control assessments. For the full text of the control, refer to IRM 10.8.1.4.4.1, CA-02 Control Assessments.
- (2) The IRS requires assessing that controls operate as intended sufficiently ensure compliance with applicable privacy requirements and manage privacy risks.
- (3) **Implementation guidance:** The IRS implements this control by assessing privacy controls via the Privacy Controls Assessment Team.
- (4) To meet this control, you must follow the policies in this IRM on the control assessments control, listed in the CA-01 references, IRM 10.5.1.8.4.
- (5) Follow the other PGLD and IRS policies that supplement the control assessments control, listed in the CA-01 references, IRM 10.5.1.8.4.

10.5.1.8.4.2
(05-08-2025)
**CA-05 Assessment
Authorization and
Monitoring — Plan of
Action and Milestones
[J] {Sys}**

- (1) This is a joint security and privacy control about plan of action and milestones (POA&Ms). For the full text of the control, refer to IRM 10.8.1.4.4.4, CA-05 Plan of Action and Milestones (POA&M).
- (2) The IRS requires monitoring privacy risks on POA&Ms per IRM 10.8.1.4.4.4 , CA-05 Plan of Action and Milestones (POA&M).
- (3) **Implementation guidance:** The IRS implements this control for privacy by requiring system owners monitor and address privacy risks identified on the PCLIA and in a privacy controls assessment in a POA&M.
- (4) To meet this control, you must follow the policies in this IRM on the plan of action and milestones control, including:

IRM	Title
IRM 10.5.1.4.4	System Owners
IRM 10.5.1.4.5	System Developers
IRM 10.5.1.4.6	Authorizing Officials

- (5) Follow the other PGLD and IRS policies that supplement the plan of action and milestones control in IRM 10.5.2.1.3, Responsibilities.

10.5.1.8.4.3
(05-08-2025)
**CA-06 Assessment
Authorization and
Monitoring —
Authorization [J] {Sys}**

- (1) This is a joint security and privacy control about authorization. For the full text of the control, refer to IRM 10.8.1.4.4.5, CA-06 Authorization.
- (2) The IRS requires addressing privacy requirements before authorization to operate.
- (3) **Implementation guidance:** The IRS implements this control by including privacy in OneSDLC (across the life cycle).
- (4) To meet this control, you must follow the policies in this IRM on the authorization control, listed in the CA-01 references, IRM 10.5.1.8.4.
- (5) Follow the other PGLD and IRS policies that supplement the authorization control, listed in the CA-01 references, IRM 10.5.1.8.4.

10.5.1.8.4.4
(05-08-2025)
**CA-07 Assessment
Authorization and
Monitoring —
Continuous Monitoring
[J] {Org}**

- (1) This is a joint security and privacy control about continuous monitoring. For the full text of the control, refer to IRM 10.8.1.4.4.6, CA-07 Continuous Monitoring.
- (2) The IRS requires staying aware of developing vulnerabilities.
- (3) **Implementation guidance:** The IRS implements this control by following privacy continuous monitoring outlined in Pub 5499, IRS Privacy Program Plan.
- (4) To meet this control, you must follow the policies in this IRM on the continuous monitoring control, listed in the CA-01 references, IRM 10.5.1.8.4.
- (5) Follow the other PGLD and IRS policies that supplement the continuous monitoring control, listed in the CA-01 references, IRM 10.5.1.8.4.

10.5.1.8.4.5
(05-08-2025)
**CA-07(4) Assessment
Authorization and
Monitoring —
Continuous Monitoring -
Risk Monitoring [J]
{Org}**

- (1) This is a joint security and privacy control about risk monitoring. For the full text of the control, refer to IRM 10.8.1.4.4.6, CA-07 Continuous Monitoring.
- (2) The IRS requires monitoring and addressing privacy risks. [Accountability; Security]
- (3) **Implementation guidance:** The IRS implements this control by monitoring risks identified in PCLIA's, privacy controls assessments, BPRAs, POA&Ms, and other assessment practices.
- (4) To meet this control, you must follow the policies in this IRM on the risk monitoring control, listed in the CA-01 references, IRM 10.5.1.8.4.
- (5) Follow the other PGLD and IRS policies that supplement the risk monitoring control, listed in the CA-01 references, IRM 10.5.1.8.4.

10.5.1.8.5
(05-08-2025)
**CM-01 Configuration
Management — Policy
and Procedures [J]
{Org}**

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the configuration management control. For the full text of the control, refer to IRM 10.8.1.4.5, CM-01 Configuration Management Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Review impacts to privacy from system changes.
 - b. Use controls to mitigate risks.
- (3) In this IRM, follow the PGLD policies on the configuration management policy and procedures control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.3	Key Privacy Concepts
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.2	Encryption
IRM 10.5.1.6.9.7	Electronic and Online

- (4) Follow the other PGLD and IRS policies that supplement the configuration management policy and procedures control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.5.1
(05-08-2025)

CM-04 Configuration Management — Impact Analysis [J] {Sys}

- (1) This is a joint security and privacy control about impact analysis. For the full text of the control, refer to IRM 10.8.1.4.5.3, CM-04 Impact Analysis.
- (2) The IRS requires determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks.
- (3) **Implementation guidance:** The IRS implements this control by reviewing Major Change Determinations (MCDs) and updating PCLIA.
- (4) To meet this control, you must follow the policies in this IRM on the impact analysis control, listed in the CM-01 references in IRM 10.5.1.8.5.
- (5) Follow the other PGLD and IRS policies that supplement the impact analysis control, listed in the CM-01 references in IRM 10.5.1.8.5.

10.5.1.8.6
(05-08-2025)

IR-01 Incident Response — Policy and Procedures [J] {Org}

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the incident response control. For the full text of the control, refer to IRM 10.8.1.4.8, IR-01 Incident Response Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Provide mandatory incident and data breach management training on how to identify and respond to a data breach.
 - b. Test the data breach response plan.
 - c. Coordinate incident and data breach handling with IM, Cyber, CSIRC, and others as needed.
 - d. Report, track, document, and plan for incidents and data breaches and responses.
 - e. Supply a support resource for incident and data breach responses.
- (3) In this IRM, follow the PGLD policies on the incident and data breach response policy and procedures control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities

IRM	Title
IRM 10.5.1.6.4	Data Loss
IRM 10.5.1.7.16	Incident Management (IM)

- (4) Follow the other PGLD and IRS policies that supplement the incident and data breach response policy and procedures control, including:

IRM or Publication	Title
IRM 10.5.4	Incident Management Program
Document 13347	Data Breach Response Playbook
Document 13347-A	IRS Data Breach Response Plan
n/a	<i>internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site</i>

10.5.1.8.6.1
(05-08-2025)
**IR-02 Incident Response
— Incident Response
Training [J] {Org}**

- (1) This is a joint security and privacy control about incident and data breach response training. For the full text of the control, refer to IRM 10.8.1.4.8.1, IR-02 Incident Response Training.
- (2) The IRS requires training on how to recognize and report an incident and data breach.
- (3) **Implementation guidance:** The IRS implements this control by providing mandatory training on incident management that is updated annually, and IM conducts a tabletop annually per OMB M-17-12.
- (4) To meet this control, you must follow the policies in this IRM on the incident and data breach response training control, listed in the IR-01 references, IRM 10.5.1.8.6.
- (5) Follow the other PGLD and IRS policies that supplement the incident and data breach response training control, including:

IRM or Publication	Title
IRM 10.5.4.2	Awareness Training and Education
n/a	<i>internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site</i>

10.5.1.8.6.2
(05-08-2025)
**IR-02(3) Incident
Response — Incident
Response Training -
Breach [P] {Org}**

- (1) Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach. [NIST SP 800-53]
- (2) The IRS requires training on how to recognize and report a data breach with PII.

- (3) **Implementation guidance:** The IRS implements this control by providing mandatory training that includes information on how to identify and respond to a data breach. The training includes links to how to respond to a data breach.
- (4) To meet this control, you must follow the policies in this IRM on the data breach control, listed in the IR-01 references, IRM 10.5.1.8.6.
- (5) Follow the other PGLD and IRS policies that supplement the data breach control, including:

IRM	Title
IRM 10.5.4.2	Awareness Training and Education
IRM 10.5.4.3	Reporting Losses, Thefts and Disclosures

10.5.1.8.6.3

(05-08-2025)

**IR-03 Incident Response
— Incident Response
Testing [J] {Org}**

- (1) This is a joint security and privacy control about incident and data breach response testing. For the full text of the control, refer to IRM 10.8.1.4.8.2, IR-03 Incident Response Testing.
- (2) The IRS requires testing incident and data breach response capabilities to verify their effectiveness and identify potential weaknesses or deficiencies.
- (3) **Implementation guidance:** The IRS implements this control by testing the data breach response plan annually following OMB M-17-12.
- (4) To meet this control, you must follow the policies in this IRM on the incident and data breach response testing control, listed in the IR-01 references, IRM 10.5.1.8.6.
- (5) Follow the other PGLD and IRS policies that supplement the incident and data breach response testing control, including:

IRM or Publication	Title
IRM 10.5.4.1.3	Responsibilities
Document 13347	Data Breach Response Playbook: Section 4.2, Tabletop Exercises: Testing the Plan
Document 13347-A	IRS Data Breach Response Plan: Section 10.1, Tabletop Exercises

10.5.1.8.6.4

(05-08-2025)

**IR-04 Incident Response
— Incident Handling [J]
{Org}**

- (1) This is a joint security and privacy control about incident and data breach handling. For the full text of the control, refer to IRM 10.8.1.4.8.3, IR-04 Incident Handling.
- (2) The IRS requires handling all incidents and data breaches consistent with the incident and data breach response plan.
- (3) **Implementation guidance:** The IRS implements this control by coordinating incident and data breach handling with IM, Cyber, CSIRC, and other business units as needed.

- (4) To meet this control, you must follow the policies in this IRM on the incident and data breach handling control, listed in the IR-01 references, IRM 10.5.1.8.6.
- (5) Follow the other PGLD and IRS policies that supplement the incident and data breach handling control, including:

IRM or Publication	Title
IRM 10.5.4.1.3	Responsibilities
Document 13347	Data Breach Response Playbook: Section 5

10.5.1.8.6.5
(05-08-2025)
IR-05 Incident Response
— Incident Monitoring
[J] {Org}

- (1) This is a joint security and privacy control about incident and data breach monitoring. For the full text of the control, refer to IRM 10.8.1.4.8.4, IR-05 Incident Monitoring.
- (2) The IRS requires tracking and documenting incidents and data breaches.
- (3) **Implementation guidance:** The IRS implements this control by using a tracking system.
- (4) To meet this control, you must follow the policies in this IRM on the incident and data breach monitoring control, listed in the IR-01 references, IRM 10.5.1.8.6.
- (5) Follow the other PGLD and IRS policies that supplement the incident and data breach monitoring control, including:

IRM or Publication	Title
IRM 10.5.4.4.1	PGLD/Incident Management Intake
Document 13347	Data Breach Response Playbook: Section 2.0, Breach Response Team (BRT); Section 3.0, Data Breach Response Process
Document 13347-A	IRS Data Breach Response Plan: Section 11.1, Tracking and Documenting the Response to a Breach

10.5.1.8.6.6
(05-08-2025)
IR-06 Incident Response
— Incident Reporting [J]
{Org}

- (1) This is a joint security and privacy control about incident and data breach reporting. For the full text of the control, refer to IRM 10.8.1.4.8.5, IR-06 Incident Reporting.
- (2) The IRS requires reporting incidents and data breaches.
- (3) **Implementation guidance:** The IRS implements this control by requiring all personnel report when an incident and data breach occurs.
- (4) To meet this control, you must follow the policies in this IRM on the incident and data breach reporting control, listed in the IR-01 references, IRM 10.5.1.8.6.

- (5) Follow the other PGLD and IRS policies that supplement the incident and data breach reporting control, including:

IRM	Title
IRM 10.5.4.3	Reporting Losses, Thefts and Disclosures
IRM 10.5.4.4.1	PGLD/Incident Management Intake

10.5.1.8.6.7

(05-08-2025)

**IR-07 Incident Response
— Incident Response
Assistance [J] {Org}**

- (1) This is a joint security and privacy control about incident and data breach response assistance. For the full text of the control, refer to IRM 10.8.1.4.8.6, IR-07 Incident Response Assistance.
- (2) The IRS requires supporting resources that offer advice and help personnel handle and report incidents and data breaches.
- (3) **Implementation guidance:** The IRS implements this control by offering a hotline.
- (4) To meet this control, you must follow the policies in this IRM on the incident and data breach response assistance control, listed in the IR-01 references, IRM 10.5.1.8.6.
- (5) Follow the other PGLD and IRS policies that supplement the incident and data breach response assistance control, including:

IRM	Title
IRM 10.5.4.1.3	Responsibilities
IRM 10.5.4.1.8	Related Resources
IRM 10.5.4.3.3	Inadvertent Unauthorized Disclosures and Losses or Thefts of IT Assets, BYOD Assets and Hardcopy Records/Documents
IRM 10.5.4.4.1	PGLD/Incident Management Intake

10.5.1.8.6.8

(05-08-2025)

**IR-08 Incident Response
— Incident Response
Plan [J] {Org}**

- (1) This is a joint security and privacy control about incident and data breach response plan. For the full text of the control, refer to IRM 10.8.1.4.8.7, IR-08 Incident Response Plan.
- (2) The IRS requires developing and implementing a coordinated approach to incident and data breach response.
- (3) **Implementation guidance:** The IRS implements this control by following Document 13347, Data Breach Response Playbook, and Document 13347-A, IRS Data Breach Response Plan.
- (4) To meet this control, you must follow the policies in this IRM on the incident and data breach response plan control, listed in the IR-01 references, IRM 10.5.1.8.6.

- (5) Follow the other PGLD and IRS policies that supplement the incident and data breach response plan control, including:

IRM or Publication	Title
IRM 10.5.4.1.3	Responsibilities
Document 13347	Data Breach Response Playbook
Document 13347-A	IRS Data Breach Response Plan

10.5.1.8.6.9
(05-08-2025)

IR-08(1) Incident Response — Incident Response Plan - Breaches [P] {Org}

- (1) Include the following in the Incident Response Plan for breaches involving personally identifiable information:
- A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
 - An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms;
 - Identification of applicable privacy requirements.
- [NIST SP 800-53]
- (2) The IRS requires developing and implementing a coordinated approach to incidents and data breaches.
- (3) **Implementation guidance:** The IRS implements this control by following Document 13347, Data Breach Response Playbook, and Document 13347-A, IRS Data Breach Response Plan.
- (4) To meet this control, you must follow the policies in this IRM on the data breaches control, listed in the IR-01 references, IRM 10.5.1.8.6.
- (5) Follow the other PGLD and IRS policies that supplement the data breaches control, including:

IRM or Publication	Title
IRM 10.5.4.3	Reporting Losses, Thefts and Disclosures
IRM 10.5.4.4.4	PGLD/Incident Management Risk Assessment and Mitigation
Document 13347	Data Breach Response Playbook
Document 13347-A	IRS Data Breach Response Plan

10.5.1.8.7
(05-08-2025)

MP-01 Media Protection — Policy and Procedures [J] {Org}

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the media protection control. For the full text of the control, refer to IRM 10.8.1.4.10 , MP-01 Media Protection Policy and Procedures.

- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
- Prevent the unauthorized disclosure of information when reusing or releasing media for disposal.
 - Follow records management and disposition and destruction requirements.
- (3) In this IRM, follow the PGLD policies on the media protection policy and procedures control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.5.1	Clean Desk Policy
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data
IRM 10.5.1.6.2	Encryption
IRM 10.5.1.6.3	Computers and Mobile Computing Devices
IRM 10.5.1.6.5	Marking
IRM 10.5.1.6.6	Storage
IRM 10.5.1.6.9	Other Forms of Transmission
IRM 10.5.1.6.10	Disposition and Destruction
IRM 10.5.1.6.15	Contracts
IRM 10.5.1.7.8	Records and Information Management (RIM)

- (4) Follow the other PGLD and IRS policies that supplement the media protection policy and procedures control, including:

IRM	Title
IRM 10.5.6.2.1	Requirements of the Privacy Act
IRM 1.15.6.11	Security of Electronic Records
IRM 1.15.6.10	Disposition of Electronic Records

10.5.1.8.7.1
(05-08-2025)

**MP-06 Media Protection
— Media Sanitization [J]
{Sys}**

- (1) This is a joint security and privacy control about media sanitization. For the full text of the control, refer to IRM 10.8.1.4.10.5, MP-06 Media Sanitization.
- (2) The IRS requires preventing the disclosure of information to unauthorized individuals when such media is reused or released for disposal.

- (3) **Implementation guidance:** The IRS implements this control by requiring proper media sanitization.
- (4) To meet this control, you must follow the policies in this IRM on the media sanitization control, including:

IRM	Title
IRM 10.5.1.6.10	Disposition and Destruction
IRM 10.5.1.7.8	Records and Information Management (RIM)

- (5) Follow the other PGLD and IRS policies that supplement the media sanitization control, including:

IRM	Title
IRM 10.5.6.2.1	Requirements of the Privacy Act
IRM 1.15.6.11	Security of Electronic Records
IRM 1.15.6.10	Disposition of Electronic Records

10.5.1.8.8
(05-08-2025)
PE-01 Physical and Environmental Protection — Policy and Procedures [J] {Org}

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the physical and environmental protection control. For the full text of the control, refer to IRM 10.8.1.4.11, PE-01 Physical and Environmental Protection Policy and Procedures.

Note: This control differs from the NIST baseline where it is a security control, but the IRS will assess it as a joint control.

- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Limit PII in visitor access records.
 - b. Minimize PII collection.
- (3) In this IRM, follow the PGLD policies on the physical and environmental protection policy and procedures control, including:

IRM	Title
IRM 10.5.1.2.11	High Security Items
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.14.3	Monitoring Individuals
IRM 10.5.1.5.1	Clean Desk Policy

- (4) Follow the other PGLD and IRS policies that supplement the physical and environmental protection policy and procedures control, including:

IRM	Title
IRM 10.5.6.2.1	Requirements of the Privacy Act
IRM 10.2.14.3	Protecting Assets
IRM 10.2.18.6	Physical Access Eligibility Requirements

10.5.1.8.8.1

(05-08-2025)

PE-08(3) Physical and Environmental Protection — Visitor Access Records - Limit Personally Identifiable Information Elements [P] {Sys}

- (1) Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: *Minimum necessary PII*. [NIST SP 800-53]
- (2) The IRS requires limiting PII elements in visitor access records when such information is not needed for operational purposes to help reduce the level of privacy risk. [Purpose Limitation; Minimizing Collection, Use, Retention, and Disclosure; Security]
- (3) **Implementation guidance:** The IRS implements this control by collecting only minimum necessary information in visitor access records.
- (4) To meet this control, you must follow the policies in this IRM on the limit personally identifiable information elements control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.14.3	Monitoring Individuals

- (5) Follow the other PGLD and IRS policies that supplement the limit personally identifiable elements control, including:

IRM	Title
IRM 10.5.6.2.1	Requirements of the Privacy Act
IRM 10.2.18.6	Physical Access Eligibility Requirements

10.5.1.8.9

(05-08-2025)

PL-01 Planning — Policy and Procedures [J] {Org}

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the planning control. For the full text of the control, refer to IRM 10.8.1.4.12, PL-01 Planning Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Include privacy in the system development lifecycle.
 - b. Communicate and document rules of behavior, including social media and external application usage restrictions.
 - c. Support privacy continuous monitoring and risk-based decision-making.

- (3) In this IRM, follow the PGLD policies on the planning policy and procedures control, including:

IRM	Title
IRM 10.5.1.3	Key Privacy Concepts
IRM 10.5.1.2.1	Privacy Lifecycle
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.11.2	Location Services
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices
IRM 10.5.1.6.17	Social Media
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.11	One Solution Delivery Life Cycle (OneSDLC)
IRM 10.5.1.7.15	IT Security

- (4) Follow the other PGLD and IRS policies that supplement the planning policy and procedures control, including:

IRM or Publication	Title
IRM 10.5.2.1.3	Responsibilities
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.2.2.5.3	Social Media PCLIA
IRM 10.5.2.3.1	FISMA Reporting
IRM 10.5.6.2.1	Requirements of the Privacy Act
IRM 10.5.6.3	Privacy Act System of Records Notices (SORNs)
IRM 10.5.5.3.1	UNAX Program Office Roles and Responsibilities
IRM 11.3.1.2	Disclosure Code, Authority and Procedure (CAP)
IRM 11.3.21.12.1	IRC 6103(k)(6) Disclosures by IRS Employees Using Social Networking and Other Internet Sites
IRM 1.15.1.3.1	Responsibilities of the IRS Records Officer
IRM 1.15.6.9	Managing Electronic Mail Records
IRM 1.15.6.11	Security of Electronic Records
IRM 1.15.6.15	Use of Social Media
IRM 11.1.3.3	Media Responsibilities
Document 12011	IRS Ethics Handbook

- 10.5.1.8.9.1
(05-08-2025)
PL-02 Planning — System Security and Privacy Plan [J] {Hybrid}
- (1) This is a joint security and privacy control about system security and privacy plan. For the full text of the control, refer to IRM 10.8.1.4.12.1, PL-02 System Security and Privacy Plan.
 - (2) The IRS requires incorporating privacy into the system development lifecycle.
 - (3) **Implementation guidance:** The IRS implements this control by following OneSDLC, completing the PCLIA process, and including privacy requirements in the system security and privacy plans.
 - (4) To meet this control, you must follow the policies in this IRM on the system security and privacy plan control, listed in the PL-01 references, IRM 10.5.1.8.9.
 - (5) Follow the other PGLD and IRS policies that supplement the system security and privacy plan control, listed in the PL-01 references, IRM 10.5.1.8.9.
- 10.5.1.8.9.2
(05-08-2025)
PL-04 Planning — Rules of Behavior [J] {Org}
- (1) This is a joint security and privacy control about rules of behavior. For the full text of the control, refer to IRM 10.8.1.4.12.3, PL-04 Rules of Behavior.
 - (2) The IRS requires following and understanding the IRS Rules of Behavior in the *internal Business Entitlement Access Request System (BEARS)* for all personnel with access to PII.
 - (3) **Implementation guidance:** The IRS implements this control by using an IRS-approved access control system [such as Business Entitlement Access Request System (BEARS)] to communicate and document acknowledgement of the IRS System Security Rules.
 - (4) To meet this control, you must follow the policies in this IRM on the rules of behavior control, including: IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities.
 - (5) Follow the other PGLD and IRS policies that supplement the rules of behavior control, including:

IRM or Publication	Title
IRM 10.5.6.2.1	Requirements of the Privacy Act
IRM 10.5.5.3.1	UNAX Program Office Roles and Responsibilities
IRM 11.3.1.2	Disclosure Code, Authority and Procedure (CAP)
Document 12011	IRS Ethics Handbook

- 10.5.1.8.9.3
(05-08-2025)
PL-04(1) Planning — Rules of Behavior - Social Media and External Site/Application Usage Restrictions [J] {Org}
- (1) This is a joint security and privacy control about social media and external site/application usage restrictions. For the full text of the control, refer to IRM 10.8.1.4.12.3, PL-04 Rules of Behavior.
 - (2) The IRS requires following and understanding the *internal Social Media Guidelines site* and the IRS Rules of Behavior in the *internal Business Entitlement Access Request System (BEARS)* for all personnel with access to PII. IRS

Communications and Liaison is responsible for external communications, and all external communications must come through their office. Refer to IRM 1.1.11.2.2 , Social Media Branch.

- (3) **Implementation guidance:** The IRS implements this control by using an IRS-approved access control system (such as BEARS) to communicate and document acknowledgement of the IRS System Security Rules.
- (4) To meet this control, you must follow the policies in this IRM on the social media and external site/application usage restrictions control, including:

IRM	Title
IRM 10.5.1.6.11.2	Location Services
IRM 10.5.1.6.17	Social Media

- (5) Follow the other PGLD and IRS policies that supplement the social media and external site/application usage restrictions control, including:

IRM or Publication	Title
IRM 10.5.2.2.5.3	Social Media PCLIA
IRM 11.1.3.3	Media Responsibilities
IRM 11.3.21.12.1	IRC 6103(k)(6) Disclosures by IRS Employees Using Social Networking and Other Internet Sites
IRM 1.15.6.15	Use of Social Media
Document 12011	IRS Ethics Handbook

10.5.1.8.9.4
(05-08-2025)
**PL-08 Planning —
Security and Privacy
Architecture [J] {Sys}**

- (1) This is a joint security and privacy control about security and privacy architecture. For the full text of the control, refer to IRM 10.8.1.4.12.7, PL-08 Security and Privacy Architecture.
- (2) The IRS requires incorporating privacy into the system development lifecycle.
- (3) **Implementation guidance:** The IRS implements this control by following OneSDLC, completing the PCLIA process, and including privacy requirements in the system security and privacy architecture.
- (4) To meet this control, you must follow the policies in this IRM on the security and privacy architecture control, listed in the PL-01 references, IRM 10.5.1.8.9.
- (5) Follow the other PGLD and IRS policies that supplement the security and privacy architecture control, listed in the PL-01 references, IRM 10.5.1.8.9.

10.5.1.8.9.5
(05-08-2025)

**PL-09 Planning —
Central Management [J]
{Org}**

- (1) This is a joint security and privacy control about central management. For the full text of the control, refer to IRM 10.8.1.4.12.8, PL-09 Central Management.

Note: This control differs from the NIST baseline where it is privacy, but joint per IRS collaboration requirements.

- (2) The IRS requires supporting privacy continuous monitoring and risk-based decision-making within the organization.
- (3) **Implementation guidance:** The IRS implements this control by managing the control assessment through the Enterprise FISMA Compliance program.
- (4) To meet this control, you must follow the policies in this IRM on the central management control, listed in the PL-01 references, IRM 10.5.1.8.9.
- (5) Follow the other PGLD and IRS policies that supplement the central management control, listed in the PL-01 references, IRM 10.5.1.8.9.

10.5.1.8.10
(05-08-2025)

**PM-01 Program
Management**

- (1) The PM-01 is a security-only [S] control in IRM 10.8.1.4.13.1, PM-01 Information Security Program Plan (InTC). We address privacy program plans separately in IRM 10.5.1.8.10.14, PM-18 Program Management — Privacy Program Plan [P] {Org}.

10.5.1.8.10.1
(05-08-2025)

**PM-03 Program
Management —
Information Security and
Privacy Resources [J]
{Org}**

- (1) This is a joint security and privacy control about information security and privacy resources. For the full text of the control, refer to IRM 10.8.1.4.13.3, PM-03 Information Security and Privacy Resources.
- (2) The IRS requires having privacy programs with the resources needed to manage federal information resources that involve PII.
- (3) **Implementation guidance:** The IRS implements this control by requiring senior management and executives make sure their programs and policies allocate sufficient resources to follow IRS privacy policies and procedures per Pub 5499, IRS Privacy Program Plan.
- (4) To meet this control, you must follow the policies in this IRM on the information security and privacy resources control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities

- (5) Follow the other PGLD and IRS policies that supplement the information security and privacy resources control, including:

IRM or Publication	Title
IRM 1.1.27.7	Program and Planning Support
Pub 5499	IRS Privacy Program Plan

10.5.1.8.10.2

(05-08-2025)

PM-04 Program Management — Plan of Action and Milestones (POA&M) Process [J] {Org}

- (1) This is a joint security and privacy control about plan of action and milestones. For the full text of the control, refer to IRM 10.8.1.4.13.4, PM-04 Plan of Action and Milestones (POA&M) Process.
- (2) The IRS requires reducing privacy risk by documenting and tracking planned remediations on POA&Ms.
- (3) **Implementation guidance:** The IRS implements this control by requiring that System Owners include privacy risks identified on the PCLIA are in a POA&M.
- (4) To meet this control, you must follow the policies in this IRM on the plan of action and milestones control, including IRM 10.5.1.4.4, System Owners.
- (5) Follow the other PGLD and IRS policies that supplement the plan of action and milestones control, including IRM 10.5.2.1.3, Responsibilities.

10.5.1.8.10.3

(05-08-2025)

PM-05(1) Program Management — System Inventory - Inventory of Personally Identifiable Information [P] {Org}

- (1) Establish, maintain, and update *annually* an inventory of all systems, applications, and projects that process personally identifiable information. [NIST SP 800-53]
- Note:** This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.
- (2) The IRS requires using this inventory to make sure that systems only process the PII for authorized purposes and that this processing is still relevant and necessary for the purpose specified. [Purpose Limitation, Security]
 - (3) **Implementation guidance:** The IRS implements this control by reviewing the PCLIA inventory at least annually.
 - (4) To meet this control, you must follow the policies in this IRM on the inventory of personally identifiable information control, including IRM 10.5.1.3.2, IRS Privacy Principles.
 - (5) Follow the other PGLD and IRS policies that supplement the inventory of personally identifiable information control, including:

IRM	Title
IRM 10.5.2.3	Reporting
IRM 10.5.6.9	Privacy Act Reports

10.5.1.8.10.4

(05-08-2025)

PM-06 Program Management — Measures of Performance [J] {Org}

- (1) This is a joint security and privacy control about measures of performance. For the full text of the control, refer to IRM 10.8.1.4.13.6, PM-06 Measures of Performance.
- (2) The IRS requires measuring the effectiveness or efficiency of the privacy programs and the controls employed.
- (3) **Implementation guidance:** The IRS implements this control by measuring privacy performance on the *internal PGLD - All Internal and External Reports site*.

- (4) To meet this control, you must follow the policies in this IRM on the measures of performance control, including:

IRM	Title
IRM 10.5.1.1.8	Program Management and Review
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.7.5	Privacy Reporting

- (5) Follow the other PGLD and IRS policies that supplement the measures of performance control, including:

IRM	Title
IRM 10.5.2.3	Reporting
IRM 10.5.4.1.4	Program Management and Review
IRM 10.5.4.4.6.3	Timeliness of the Data Breach Notification
IRM 11.3.13.1.4	Program Management and Review
IRM 11.3.13.8	FOIA Reporting
IRM 11.3.39.1.5	Program Controls

10.5.1.8.10.5
(05-08-2025)

**PM-07 Program
Management —
Enterprise Architecture
[J] {Org}**

- (1) This is a joint security and privacy control about enterprise architecture. For the full text of the control, refer to IRM 10.8.1.4.13.7, PM-07 Enterprise Architecture.
- (2) The IRS requires protecting privacy throughout the solution development life cycle.
- (3) **Implementation guidance:** The IRS implements this control by requiring compliance with Enterprise Architecture's standards.
- (4) To meet this control, you must follow the policies in this IRM on the enterprise architecture control, including:

IRM	Title
IRM 10.5.1.3	Key Privacy Concepts
IRM 10.5.1.7.11	One Solution Delivery Life Cycle (OneSDLC)

- (5) Follow the other PGLD and IRS policies that supplement the enterprise architecture control, including:

IRM	Title
IRM 10.5.2.1.1	Background

IRM	Title
IRM 10.5.2.2.4	System PCLIA's
IRM 10.5.2.2.4.7	Reconciliation with As-Built Architecture (ABA)

10.5.1.8.10.6
(05-08-2025)

**PM-08 Program
Management — Critical
Infrastructure Plan [J]
{Org}**

- (1) This is a joint security and privacy control about critical infrastructure plan. For the full text of the control, refer to IRM 10.8.1.4.13.8, PM-08 Critical Infrastructure Plan.
- (2) The IRS requires addressing privacy issues in critical infrastructure, assets, resources, and processes in the mission life cycle.
- (3) **Implementation guidance:** The IRS implements this control by embedding data protection through the life cycle of critical infrastructure, assets, resources, and processes.
- (4) To meet this control, you must follow the policies in this IRM on the critical infrastructure plan control, including:

IRM	Title
IRM 10.5.1.2.1	Privacy Lifecycle
IRM 10.5.1.2.2	Sensitive But Unclassified (SBU) Data

- (5) Follow the other PGLD and IRS policies that supplement the critical infrastructure plan control, including:

IRM	Title
IRM 10.5.2.2.2	PCLIA's Relevance to Privacy Compliance
IRM 10.6.1.1.3	Responsibilities

10.5.1.8.10.7
(05-08-2025)

**PM-09 Program
Management — Risk
Management Strategy [J]
{Org}**

- (1) This is a joint security and privacy control about risk management strategy. For the full text of the control, refer to IRM 10.8.1.4.13.9, PM-09 Risk Management Strategy.
- (2) The IRS requires managing privacy risk to individuals resulting from the authorized processing of PII. [Accountability; Minimizing Collection, Use, Retention, and Disclosure; Strict Confidentiality]
- (3) **Implementation guidance:** The IRS implements this control by:
 - a. Implementing a risk management framework consistent with OMB guidance.
 - b. Assessing regularly for risks based on the privacy controls.
 - c. Developing and monitoring mitigation projects to minimize privacy risks.
- (4) To meet this control, you must follow the policies in this IRM on the risk management strategy control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.3.1	Privacy Controls
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.1.1	Deciding Risk Levels for SBU Data
IRM 10.5.1.6.18.4	Cloud Computing
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.3	Business PII Risk Assessment (BPRA)
IRM 10.5.1.7.10	Digital Identity Risk Assessment (DIRA)
IRM 10.5.1.7.14.2	Non-Digital Authentication Risk Assessment (NDARA)

- (5) Follow the other PGLD and IRS policies that supplement the risk management strategy control, including:

IRM or Publication	Title
IRM 10.5.2.1.3	Responsibilities
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.2.2.4.3	Major Change Determination (MCD) for PCLIA
IRM 10.5.2.4	Business PII Risk Assessment (BPRA)
IRM 10.5.4.4.4	PGLD/Incident Management Risk Assessment and Mitigation
IRM 10.5.5.3	Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
IRM 10.5.6.2.9	OMB Privacy Act Guidance
IRM 10.5.6-1	Agency Review Requirements
Pub 5499	IRS Privacy Program Plan

10.5.1.8.10.8
(05-08-2025)
**PM-10 Program
Management —
Authorization Process
[J] {Org}**

- (1) This is a joint security and privacy control about authorization process. For the full text of the control, refer to IRM 10.8.1.4.13.10, PM-10 Authorization Process.
- (2) The IRS requires addressing privacy requirements before authorization to operate.
- (3) **Implementation guidance:** The IRS implements this control by including privacy in OneSDLC (across the life cycle).
- (4) To meet this control, you must follow the policies in this IRM on the authorization process control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.3.1	Privacy Controls
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.18.4	Cloud Computing
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.3	Business PII Risk Assessment (BPRA)
IRM 10.5.1.7.10	Digital Identity Risk Assessment (DIRA)
IRM 10.5.1.7.14.2	Non-Digital Authentication Risk Assessment (NDARA)

- (5) Follow the other PGLD and IRS policies that supplement the authorization process control, including:

IRM or Publication	Title
IRM 10.5.2.1.3	Responsibilities
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.2.2.4.3	Major Change Determination (MCD) for PCLIA
IRM 10.5.2.4	Business PII Risk Assessment (BPRA)
IRM 10.5.4.4.4	PGLD/Incident Management Risk Assessment and Mitigation
IRM 10.5.5.3	Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
IRM 10.5.6.2.9	OMB Privacy Act Guidance
IRM 10.5.6-1	Agency Review Requirements
Pub 5499	IRS Privacy Program Plan

10.5.1.8.10.9
(05-08-2025)

**PM-11 Program
Management — Mission
and Business Process
Definition [J] {Org}**

- (1) This is a joint security and privacy control about mission and business process definition. For the full text of the control, refer to IRM 10.8.1.4.13.11, PM-11 Mission and Business Process Definition.
- (2) The IRS requires protecting privacy in systems and safeguards privacy in everyday business processes supporting the IRS mission. [Accountability]
- (3) **Implementation guidance:** The IRS implements this control by requiring a privacy culture, where all personnel think about privacy before acting. The mission of the service requires the IRS safeguard privacy and protect privacy rights.
- (4) To meet this control, you must follow the policies in this IRM on the mission and business process definition control, including:

IRM	Title
IRM 10.5.1.1.1	Purpose of the Program
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.5	Privacy Culture

- (5) Follow the other PGLD and IRS policies that supplement the mission and business process definition control, including:

IRM or Publication	Title
IRM 10.5.2.4	Business PII Risk Assessment (BPRA)
IRM 10.5.6.1.3	Roles and Responsibilities
IRM 10.5.6.2.7	IRS Privacy Principles
IRM 11.3.1.2	Disclosure Code, Authority and Procedure (CAP)
IRM 1.1.27.1.4	Roles and Responsibilities
IRM 1.2.1.2.1	Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights
IRM 1.2.1.17.2	Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safeguarding Confidential Tax Information
Pub 5499	IRS Privacy Program Plan

10.5.1.8.10.10
(05-08-2025)

**PM-13 Program
Management — Security
and Privacy Workforce
[J] {Org}**

- (1) This is a joint security and privacy control about security and privacy workforce. For the full text of the control, refer to IRM 10.8.1.4.13.13, PM-13 Security and Privacy Workforce.
- (2) The IRS requires developing and institutionalizing the core privacy capabilities of personnel needed to protect organizational operations, assets, and individuals. [Privacy Awareness and Training]
- (3) **Implementation guidance:** The IRS implements this control by defining and developing privacy training for PGLD and other privacy-minded personnel.
- (4) To meet this control, you must follow the policies in this IRM on the security and privacy workforce control, including:

IRM	Title
IRM 10.5.1.1.2	Audience
IRM 10.5.1.3.2	IRS Privacy Principles

- (5) Follow the other PGLD and IRS policies that supplement the security and privacy workforce control, including:

IRM or Publication	Title
IRM 10.5.2.2.3	PCLIA Roles and Responsibilities
IRM 10.5.6.2.8	Privacy Act Training
IRM 1.1.27.1.4	Roles and Responsibilities
Pub 5499	IRS Privacy Program Plan

10.5.1.8.10.11
(05-08-2025)

**PM-14 Program
Management — Testing,
Training, and Monitoring
[J] {Org}**

- (1) This is a joint security and privacy control about testing, training, and monitoring. For the full text of the control, refer to IRM 10.8.1.4.13.14, PM-14 Testing, Training, and Monitoring.
- (2) The IRS requires coordinating the training for personnel with access to PII and the testing of privacy controls. [Privacy Awareness and Training]
- (3) **Implementation guidance:** The IRS implements this control by reviewing testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
- (4) To meet this control, you must follow the policies in this IRM on the testing, training, and monitoring control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data
IRM 10.5.1.6.15	Contracts
IRM 10.5.1.7.7	Mandatory Briefings

- (5) Follow the other PGLD and IRS policies that supplement the testing, training, and monitoring control, including:

IRM or Publication	Title
IRM 10.5.2.1	Program Scope and Objectives
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.4.1	Program Scope and Objectives
IRM 10.5.4.1.3	Responsibilities
IRM 10.5.4.2	Awareness Training and Education
IRM 10.5.5.3	Service-wide Roles and Responsibilities for Administering the IRS UNAX Program
IRM 10.5.6.2.8	Privacy Act Training

IRM or Publication	Title
IRM 11.3.1.1.3	Roles and Responsibilities
IRM 1.15.1.1.3	Responsibilities
IRM 1.15.1.3	Oversight Responsibilities
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.10.12
(05-08-2025)

**PM-15 Program
Management — Security
and Privacy Groups and
Associations [J] {Org}**

- (1) This is a joint security and privacy control about security and privacy groups and associations. For the full text of the control, refer to IRM 10.8.1.4.13.15, PM-15 Security and Privacy Groups and Associations.

Note: This control differs from the NIST baseline where it is a security control, but the IRS will assess it as a joint control.

- (2) The IRS requires ongoing contact with security and privacy groups and associations in an environment of rapidly changing technologies and threats.
- (3) **Implementation guidance:** The IRS implements this control by encouraging participation in appropriate groups, such as the Federal Privacy Council (FPC) and International Association of Privacy Professionals (IAPP).
- (4) To meet this control, you must follow the policies in this IRM on the security and privacy groups and associations control, including:

IRM	Title
IRM 10.5.1.7.1	IRS Privacy Council
Exhibit 10.5.1-2	References

- (5) Follow the other PGLD and IRS policies that supplement the security and privacy groups and associations control, including:

IRM or Publication	Title
IRM 1.1.27.1.4	Roles and Responsibilities
Pub 5499	IRS Privacy Program Plan

10.5.1.8.10.13
(05-08-2025)

**PM-17 Program
Management —
Protecting Controlled
Unclassified Information
on External Systems [J]
{Org}**

- (1) This is a joint security and privacy control about protecting controlled unclassified information (CUI) on external systems. For the full text of the control, refer to IRM 10.8.1.4.13.17, PM-17 Protecting Controlled Unclassified Information on External Systems.
- (2) The IRS requires protecting all sensitive information on external systems by partners following the privacy policy in IRM 10.5.1.6.15, Contracts. This means

including all privacy requirements language in all contracts, with few approved exceptions. [NIST SP 800-171]

- (3) **Implementation guidance:** The IRS uses SBU data to describe what this control calls CUI. The IRS implements this control by requiring that contractors, subcontractors, and external partners protect all SBU data (including PII and tax information). This means all IRS acquisitions and agreements must include language holding contractors, subcontractors, and other service providers accountable for following federal and IRS privacy policies and procedures. Examples of such policies include privacy requirements language in contracts, PCLIAs for contracted IT, security and privacy controls, and defining contractors as IRS personnel in this IRM with all the same responsibilities for data protection.

Note: Once the IRS implements the CUI program, these requirements will apply to all CUI just as they do to SBU data today.

- (4) To meet this control, you must follow the policies in this IRM on the protecting controlled unclassified information (SBU data) on external systems control, including:

IRM	Title
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.15	Contracts
IRM 10.5.1.6.18.4	Cloud Computing
IRM 10.5.1.7.12	Governmental Liaison (GL)
IRM 10.5.1.7.18	Safeguards

- (5) Follow the other PGLD and IRS policies that supplement the protecting controlled unclassified information (SBU data) on external systems control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.4.3	Reporting Losses, Thefts, and Disclosures
IRM 10.5.5.3.4	Contracting Officer's Representative (COR) UNAX Responsibilities
IRM 10.5.5.3.5	Employee UNAX Responsibilities
IRM 10.5.6.1.3	Roles and Responsibilities
IRM 10.5.6.2.8	Privacy Act Training
IRM 10.5.6.2.9.1	Privacy Act Contract Requirements
IRM 11.3.24.2	Requirements
IRM 11.3.36.2	Legal Requirements

IRM or Publication	Title
IRM 11.4.1.13	Procedures for Routing, Approving, Signing and Terminating Basic Agreements (BAs), Implementing Agreements (IAs), Memorandums of Understanding (MOUs), and Other Agreements
IRM 1.15.1.1.3	Responsibilities
Pub 4812	Contractor Security & Privacy Controls
Pub 1075	Tax Information Security Guidelines for Federal, State and Local Agencies
Document 13347	Data Breach Response Playbook: Section 5.4, External Third-Party Incidents
Document 13347-A	IRS Data Breach Response Plan: Section 2.5, Contractors
n/a	<i>internal IRS Acquisition Policy (IRSAP) site Index C (pdf)</i>

10.5.1.8.10.14
(05-08-2025)

**PM-18 Program
Management — Privacy
Program Plan [P] {Org}**

- (1) Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:
 - a. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;
 - b. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
 - c. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
 - d. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;
 - e. Reflects coordination among organizational entities responsible for the different aspects of privacy; and
 - f. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and
 - (2) Update the plan *every three years or more often to address changes* in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments. [NIST SP 800-53]
- Note:** This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.
- (3) The IRS requires documenting its privacy program formally.
 - (4) **Implementation guidance:** The IRS implements this control by publishing Pub 5499, IRS Privacy Program Plan.
 - (5) To meet this control, you must follow the policies in this IRM on the Privacy Program Plan control, including:

IRM	Title
IRM 10.5.1.1	Program Scope and Objectives
IRM 10.5.1.3.1	Privacy Controls

- (6) Follow the other PGLD and IRS policies that supplement the Privacy Program Plan control, including:

IRM or Publication	Title
IRM 10.5.6.2.9	OMB Privacy Act Guidance
Pub 5499	IRS Privacy Program Plan

10.5.1.8.10.15
(05-08-2025)
**PM-19 Program
Management — Privacy
Program Leadership
Role [P] {Org}**

- (1) Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program. [NIST SP 800-53]

Note: This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.

- (2) The IRS requires having a senior official responsible for making sure the IRS implements sound policies to protect SBU data (including PII and tax information).
- (3) **Implementation guidance:** The IRS implements this control by having a Chief Privacy Officer (CPO); Treasury appoints the senior agency official for privacy (SAOP).
- (4) To meet this control, you must follow the policies in this IRM on the privacy program leadership role control, including:

IRM	Title
IRM 10.5.1.1.1	Purpose of the Program
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.7.1	IRS Privacy Council

- (5) Follow the other PGLD and IRS policies that supplement the privacy program leadership role control, including:

IRM or Publication	Title
IRM 10.5.6.1.3	Roles and Responsibilities
IRM 10.5.6.2.9	OMB Privacy Act Guidance
IRM 1.1.27.1.4	Roles and Responsibilities

IRM or Publication	Title
Pub 5499	IRS Privacy Program Plan

10.5.1.8.10.16
(05-08-2025)

**PM-20 Program
Management —
Dissemination of Privacy
Program Information [P]
{Org}**

- (1) Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that:
 - a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;
 - b. Ensures that organizational privacy practices and reports are publicly available; and
 - c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

[NIST SP 800-53]

Note: This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.

- (2) The IRS requires publishing information so people have a way to review privacy policies and contact the IRS about concerns.
- (3) **Implementation guidance:** The IRS implements this control by maintaining the *IRS.gov Privacy Policy (external)* page with all required elements following IRM 10.5.1.6.16.1, IRS.gov Privacy Policy Notice, including a link to the Treasury SAOP contact information.
- (4) To meet this control, you must follow the policies in this IRM on the dissemination of privacy program information control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices

- (5) Follow the other PGLD and IRS policies that supplement the dissemination of privacy program information control, including:

IRM or Publication	Title
IRM 10.5.2.2.4.5	PCLIAs on IRS.gov
IRM 10.5.6.3	Privacy Act System of Records Notices (SORNs)
IRM 10.5.6.6	Privacy Act Requests for Non-Tax Records
IRM 11.3.7	Freedom of Information Act Reading Room Operations
IRM 11.3.13	Freedom of Information Act

IRM or Publication	Title
Pub 5499	IRS Privacy Program Plan
n/a	<i>IRS.gov Privacy Policy (external)</i>

10.5.1.8.10.17
(05-08-2025)

PM-20(1) Program Management — Dissemination of Privacy Program Information - Privacy Policies on Websites, Applications, and Digital Services [P] {Org}

- (1) Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:

- Are written in plain language and organized in a way that is easy to understand and navigate;
- Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and
- Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

[NIST SP 800-53]

Note: This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.

- (2) The IRS requires allowing the public to make an informed decision about sharing their information. [Openness and Consent]
- (3) **Implementation guidance:** The IRS implements this control by both maintaining the IRS.gov Privacy Policy page *IRS.gov Privacy Policy (external)* with all required elements following IRM 10.5.1.6.16.1, IRS.gov Privacy Policy Notice, and a link to that page for all external facing online services.
- (4) To meet this control, you must follow the policies in this IRM on the privacy policies on the websites, applications, and digital services control, including:

IRM or Publication	Title
IRM 10.5.1.3.2.4	Openness and Consent
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices
n/a	<i>IRS.gov Privacy Policy (external)</i>

- (5) Follow the other PGLD and IRS policies that supplement the privacy policies on the websites, applications, and digital services control, including:

IRM or Publication	Title
IRM 10.5.6.4.6	Online Privacy Policy Notices
IRM 10.5.6.5	Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)
n/a	<i>IRS.gov Privacy Policy (external)</i>

10.5.1.8.10.18
(05-08-2025)
**PM-21 Program
Management —
Accounting of
Disclosures [P] {Org}**

- (1) Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:
 - a. Date, nature, and purpose of each disclosure; and
 - b. Name and address, or other contact information of the individual or organization to which the disclosure was made;
- (2) Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and
- (3) Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request. [NIST SP 800-53]

Note: This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.

- (4) The IRS requires allowing individuals to learn to whom the IRS disclosed their non-tax Privacy Act records. [Accountability; Access, Correction, and Redress]
- (5) **Implementation guidance:** The IRS implements this control by requiring that employees authorized to make disclosures of non-tax Privacy Act records account for such disclosures following IRM 10.5.6.7, Privacy Act Accounting of Disclosures .
- (6) To meet this control, you must follow the policies in this IRM on the accounting of disclosures control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.2.7	Privacy Act Information

- (7) Follow the other PGLD and IRS policies that supplement the accounting of disclosures control, including:

IRM	Title
IRM 10.5.6.7	Privacy Act Accounting of Disclosures
IRM 11.3.37.3	Accounting System
IRM 6.711.2.8	Analyzing/Processing the Request
IRM 6.751.1-9	TIGTA Cases
IRM 4.36.4.11	Disclosure of Individual Information — Form 5482, Record of Disclosure
IRM 8.7.9.6.8	Disclosure Provisions for JC Cases - Form 5482

10.5.1.8.10.19

(05-08-2025)

PM-22 Program Management — Personally Identifiable Information Quality Management [P] {Org}

- (1) Develop and document organization-wide policies and procedures for:
 - a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;
 - b. Correcting or deleting inaccurate or outdated personally identifiable information;
 - c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and
 - d. Appeals of adverse decisions on correction or deletion requests.

[NIST SP 800-53]

Note: This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.

- (2) The IRS requires confirming the accuracy and relevance of PII throughout the information life cycle. [Data Quality, Verification and Notification]
- (3) **Implementation guidance:** The IRS implements this control by requiring those who process PII to confirm the accuracy, completeness, and timeliness of PII to ensure fair treatment of all individuals. IRS personnel must collect information, to the greatest extent practical, directly from the individual to whom it relates.
- (4) To meet this control, you must follow the policies in this IRM on the personally identifiable information quality management control, including:

IRM	Title
IRM 10.5.1.2.1	Privacy Lifecycle
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.14	Civil Liberties

- (5) Follow the other PGLD and IRS policies that supplement the personally identifiable information quality management control, including:

IRM	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.6.1	Program Scope and Objectives
IRM 10.5.6.2	Privacy Act General Provisions
IRM 10.5.6.5	Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)
IRM 10.5.6.5	Privacy Act Requests for Non-Tax Records

10.5.1.8.10.20
(05-08-2025)
**PM-23 Program
Management — Data
Governance Body [J]
{Org}**

- (1) This is a joint security and privacy control about data governance body. For the full text of the control, refer to IRM 10.8.1.4.13.23, PM-23 Data Governance Body.

Note: This control differs from the NIST baseline where it is a security control, but the IRS will assess it as a joint control.

- (2) The IRS requires managing data, including PII, following applicable laws, executive orders, directives, regulations, policies, standards, and guidance. [Accountability; Data Quality]
- (3) **Implementation guidance:** The IRS implements this control by using the IRS Privacy Council, Data Security Executive Steering Committee, Cybersecurity and Privacy Governance Board, and other oversight to establish policies, procedures, and standards that help data governance.
- (4) To meet this control, you must follow the policies in this IRM on the data governance body control, including:

IRM	Title
IRM 10.5.1.1.6	Authority
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.7	Privacy-Related Programs

- (5) Follow the other PGLD and IRS policies that supplement the data governance body control, including:

IRM	Title
IRM 10.5.6.9.4	Annual Matching Activity Review and Report
IRM 11.3.39.1.4	Program Management and Review
IRM 2.173.1	IT Governance Policy
IRM 2.173.2	IT Governance Procedures

10.5.1.8.10.21
(05-08-2025)
**PM-24 Program
Management — Data
Integrity Board [P] {Org}**

- (1) Establish a Data Integrity Board to:
- Review proposals to conduct or participate in a matching program; and
 - Conduct an annual review of all matching programs in which the agency has participated.

[NIST SP 800-53]

Note: This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.

- (2) The IRS requires monitoring its computer matching activities. [Data Quality]
- (3) **Implementation guidance:** The IRS implements this control with the CPO representing the IRS as a member of the Treasury Data Integrity Board.

- (4) To meet this control, you must follow the policies in this IRM on the data integrity board control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.1.2	Limiting Sharing of SBU Data
IRM 10.5.1.7.13	Data Services

- (5) Follow the other PGLD and IRS policies that supplement the data integrity board control, including:

IRM	Title
IRM 10.5.6.9.4	Annual Matching Activity Review and Report
IRM 11.3.39.1.4	Program Management and Review

10.5.1.8.10.22
(05-08-2025)
PM-25 Program Management — Minimization of Personally Identifiable Information Used for Testing, Training, and Research [P] {Org}

- (1) Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;
 - (2) Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;
 - (3) Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
 - (4) Review and update policies and procedures *every three years or when a significant change*. [NIST SP 800-53]
- Note:** This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.
- (5) The IRS requires minimizing or fictionalizing PII with synthetic data in testing, research, and training because PII increases the risk of unauthorized disclosure or misuse of such information. {Minimizing Collection, Use, Retention, and Disclosure}
 - (6) **Implementation guidance:** The IRS implements this control by requiring the SBU Data Use process for non-production environments and fictionalization of SBU data in training and research.
 - (7) To meet this control, you must follow the policies in this IRM on the minimization of personally identifiable information used for testing, training, and research control, including:

IRM	Title
IRM 10.5.1.3.2.3	Minimizing Collection, Use, Retention, and Disclosure

IRM	Title
IRM 10.5.1.6.19	Training
IRM 10.5.1.7.20	SBU Data Use for Non-Production Environments

- (8) Follow the other PGLD and IRS policies that supplement the minimization of personally identifiable information used for testing, training, and research control, including:

IRM or Publication	Title
IRM 10.5.8	Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments
Document 13324	Guidelines and Examples for Fictionalizing Domestic Taxpayer Information
Document 13311	International Name and Address Construction Job Aid
IRM 6.410.1.3.10	Disclosure Requirements
IRM 6.410.1.3.11	Ethics and Privacy
IRM 6.410.1.3.12	Personally Identifiable Information (PII)
IRM 2.12.2.26	RMODE - Research mode

10.5.1.8.10.23
(05-08-2025)
**PM-26 Program
Management —
Complaint Management
[P] {Org}**

- (1) Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:
- Mechanisms that are easy to use and readily accessible by the public;
 - All information necessary for successfully filing complaints;
 - Tracking mechanisms to ensure all complaints received are reviewed and addressed (*and resolved*) *within 20 business days of receipt*;
 - Acknowledgement of receipt of complaints, concerns, or questions from individuals *in writing, if the IRS will not be resolving the complaint within the 20 business days of receipt*; and
 - Response to complaints, concerns, or questions from individuals *to fully resolve the complaint within 20 business days of receipt*.

[NIST SP 800-53]

Note: This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.

- (2) The IRS requires responding to concerns that members of the public and employees might have about their privacy by following the *internal Management of Privacy Complaints and Inquiries SOP document*. [Access, Correction, and Redress]
- (3) **Implementation guidance:** The IRS implements this control with:
- The *internal Management of Privacy Complaints and Inquiries SOP document*.

- IRM 10.5.6.6.5, Privacy Complaints.
- The Privacy Complaints section on *IRS.gov Privacy Policy (external)*.

- (4) To meet this control, you must follow the policies in this IRM on the complaint management control, including:

IRM	Title
IRM 10.5.1.1.1	Purpose of the Program
IRM 10.5.1.3.2.9	Access, Correction, and Redress
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices
IRM 10.5.1.7.5	Privacy Reporting

- (5) Follow the other PGLD and IRS policies that supplement the complaint management control, including:

IRM or Publication	Title
IRM 10.5.2.3.2	Section 803 Reporting
IRM 10.5.6.1.3	Roles and Responsibilities
IRM 10.5.6.6.5	Privacy Complaints
Pub 5499	IRS Privacy Program Plan
n/a	<i>IRS.gov/privacy (IRS Privacy Policy)(external)</i>

10.5.1.8.10.24
(05-08-2025)
**PM-27 Program
Management — Privacy
Reporting [P] {Org}**

- (1) Develop all required privacy reports listed in the latest spreadsheet for internal and external reports on the *internal PGLD - All Internal and External Reports site* and disseminate to:
- the appropriate oversight bodies in the Distribution Level(s) column* to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and
 - the appropriate officials in the Groups Responsible column* and other personnel with responsibility for monitoring privacy program compliance; and
- (2) Review and update privacy reports *on the frequency listed in the Due Date column*. [NIST SP 800-53]

Note: This control differs from the NIST baseline where it is a joint control, but the IRS will assess it as a privacy control.

- (3) The IRS requires promoting accountability and transparency in organizational privacy operations. [Openness and Consent]
- (4) **Implementation guidance:** The IRS implements this control by following existing reporting activities.
- (5) To meet this control, you must follow the policies in this IRM on the privacy reporting control, including:

IRM	Title
IRM 10.5.1.3.2.4	Openness and Consent
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices
IRM 10.5.1.7.5	Privacy Reporting

- (6) Follow the other PGLD and IRS policies that supplement the privacy reporting control, including:

IRM or Publication	Title
IRM 10.5.2.3	Reporting
IRM 10.5.4.1.4	Program Management and Review
IRM 10.5.4.4.6.3	Timeliness of the Data Breach Notification
IRM 10.5.4.4.2	High-Risk Data Breaches
IRM 10.5.5.3	Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
IRM 10.5.6.9	Privacy Act Reports
IRM 11.3.13.8	FOIA Reporting
IRM 11.3.37.4	Disclosure Accounting Report to the Joint Committee on Taxation (JCT)
IRM 11.3.39.5.2	Matching Program Notice and Reporting Requirements
Document 13347-A	IRS Data Breach Response Plan: Section 11, Reports
n/a	<i>Internal PGLD - All Internal and External Reports site</i>
n/a	<i>IRS.gov/privacy (IRS Privacy Policy)(external)</i>

10.5.1.8.10.25
(05-08-2025)
**PM-28 Program
Management — Risk
Framing [J] {Org}**

- (1) This is a joint security and privacy control about risk framing. For the full text of the control, refer to IRM 10.8.1.4.13.28, PM-28 Risk Framing.
- (2) The IRS requires informing risk assessment, risk response, and risk monitoring activities with privacy. [Accountability; Security]
- (3) **Implementation guidance:** The IRS implements this control by conducting PCLIAAs, BPRAs, and other risk assessment, response, and monitoring activities and sharing results with the CPO.
- (4) To meet this control, you must follow the policies in this IRM on the risk framing control, including:

IRM	Title
IRM 10.5.1.1.5	Background
IRM 10.5.1.3.2	IRS Privacy Principles

IRM	Title
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data and PII
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.3	Business PII Risk Assessment (BPRA)
IRM 10.5.1.7.10	Digital Identity Risk Assessment (DIRA)

- (5) Follow the other PGLD and IRS policies that supplement the risk framing control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.2.4	Business PII Risk Assessment (BPRA)
IRM 10.5.4.1.1	Background
IRM 10.5.4.1.3	Responsibilities
IRM 10.5.4.4.1	PGLD/Incident Management Intake
IRM 10.5.4.4.4	PGLD/Incident Management Risk Assessment and Mitigation
IRM 10.10.1.7	Oversight Procedure
Pub 5499	IRS Privacy Program Plan

10.5.1.8.10.26
(05-08-2025)

**PM-31 Program
Management —
Continuous Monitoring
Strategy [J] {Org}**

- (1) This is a joint security and privacy control about continuous monitoring strategy. For the full text of the control, refer to IRM 10.8.1.4.13.31, PM-31 Continuous Monitoring Strategy.
- (2) The IRS requires conducting continuous monitoring to support organizational risk management decisions in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. [Accountability; Security]
- (3) **Implementation guidance:** The IRS implements this control by following its continuous monitoring strategy outlined in Pub 5499, IRS Privacy Program Plan.
- (4) To meet this control, you must follow the policies in this IRM on the continuous monitoring strategy control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.3.1	Privacy Controls

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.18.4	Cloud Computing
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.3	Business PII Risk Assessment (BPRA)
IRM 10.5.1.7.10	Digital Identity Risk Assessment (DIRA)
IRM 10.5.1.7.14.2	Non-Digital Authentication Risk Assessment (NDARA)

- (5) Follow the other PGLD and IRS policies that supplement the continuous monitoring strategy control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.2.4	Business PII Risk Assessment (BPRA)
IRM 10.5.4.4.4	PGLD/Incident Management Risk Assessment and Mitigation
IRM 10.5.5.3	Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
IRM 10.5.6.2.9	OMB Privacy Act Guidance
IRM 10.5.6-1	Agency Review Requirements
Pub 5499	IRS Privacy Program Plan

10.5.1.8.11
(05-08-2025)
**PS-01 Personnel
Security — Policy and
Procedures [J] {Org}**

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the personnel security policy and procedures control. For the full text of the control, refer to IRM 10.8.1.4.14, PS-01 Personnel Security Policy and Procedures.

Note: This control differs from the NIST baseline where it is a security control, but the IRS will assess it as a joint control.

- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to understand the rules of behavior through access agreements.
- (3) In this IRM, follow the PGLD policies on the personnel security policy and procedures control, including:

IRM	Title
IRM 10.5.1.1.2	Audience
IRM 10.5.1.2.8	Need To Know

IRM	Title
IRM 10.5.1.2.10	Authorization
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.15	Contracts

- (4) Follow the other PGLD and IRS policies that supplement the personnel security policy and procedures control, including:

IRM or Publication	Title
IRM 10.5.5.1.5	Program Controls
IRM 10.23 series	Personnel Security
Pub 4812	Contractor Security & Privacy Controls

10.5.1.8.11.1
(05-08-2025)

PS-06 Personnel Security — Access Agreements [J] {Org}

- (1) This is a joint security and privacy control about access agreements. For the full text of the control, refer to IRM 10.8.1.4.14.5, PS-06 Access Agreements.
- (2) The IRS requires having access agreements so all personnel with access to PII understand the IRS Rules of Behavior in the *internal Business Entitlement Access Request System (BEARS)*. [Accountability]
- (3) **Implementation guidance:** The IRS implements this control by using an IRS-approved access control system (such as BEARS) to communicate and document acknowledgement of the IRS System Security Rules (which serves as the access agreement).
- (4) To meet this control, you must follow the policies in this IRM on the access agreements control in the PS-01 references, IRM 10.5.1.8.11.
- (5) Follow the other PGLD and IRS policies that supplement the access agreements control in the PS-01 references, IRM 10.5.1.8.11.

10.5.1.8.12
(05-08-2025)

PT-01 Personally Identifiable Information Processing and Transparency — Policy and Procedures [P] {Org}

- (1) Develop, document, and disseminate to *all IRS personnel with access to PII*:
 - a. *Organization-level (IRM 10.5.1, Privacy Policy, and IRM 10.5.6, Privacy Act)* personally identifiable information processing and transparency policy that:
 1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 - b. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;

- (2) Designate *the CPO or designee* to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and
- (3) Review and update the current personally identifiable information processing and transparency:
 - a. Policy *every three years* and following *significant changes in federal privacy laws and policy*; and
 - b. Procedures *every three years* and following *significant changes in federal privacy laws and policy*.

[NIST SP 800-53]

- (4) **Implementation guidance:** The IRS implements this control with current policies in IRM 10.5.1, Privacy Policy, and IRM 10.5.6, Privacy Act, that address this control family's concerns and require personnel to:
 - a. Protect PII from unauthorized access, use, and disclosure.
 - b. Limit use of PII to the published authorities and purposes, with notice and consent as required by law.
 - c. Apply all relevant IRS privacy policy protections for specific categories of PII, including limiting the unnecessary use of SSNs and restricting the unauthorized collection of First Amendment information.

Note: If IRM 10.5.1 and other IRM sections conflict, the more restrictive requirement prevails.

- (5) In this IRM, follow the PGLD policies on the personally identifiable information processing and transparency policy and procedures control, including:

IRM	Title
IRM 10.5.1	Privacy Policy (and all subsections)

- (6) Follow the other PGLD and IRS policies that supplement the personally identifiable information processing and transparency policy and procedures control, including:

IRM	Title
IRM 10.5.6	Privacy Act (and all subsections)
IRM 10.5.2	Privacy Compliance and Assurance (PCA) Program (and all subsections)
IRM 10.5.4	Incident Management Program (and all subsections)
IRM 10.5.5	Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements (and all subsections)
IRM 10.5.7	Use of Pseudonyms by IRS Employees (and all subsections)
IRM 10.5.8	Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments (and all subsections)
IRM 1.15 series	Records and Information Management (all sections and subsections)

IRM	Title
IRM 11.3 series	Disclosure of Official Information (all sections and subsections)
IRM 1.2.1.2.1	Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights
IRM 1.2.1.17.2	Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safeguarding Confidential Tax Information
various	The more than 200 other IRS IRMs that include policy referencing PII.

10.5.1.8.12.1
(05-08-2025)

PT-02 Personally Identifiable Information Processing and Transparency — Authority to Process Personally Identifiable Information [P] {Org}

- (1) Determine and document the *organizational-level Internal Revenue Code (IRC), Privacy Act, or other legal authority* that permits the *processing* of personally identifiable information; and
- (2) Restrict the *processing* of personally identifiable information to only that which is authorized. [NIST SP 800-53]
- (3) The IRS requires processing PII only for authorized purposes. [Purpose Limitation]
- (4) **Implementation guidance:** The IRS implements this control by following the IRS Privacy Principle of Purpose Limitation and documenting authority – before information collection – in SORNs, privacy policies and notices, PCLIAs, Privacy Act statements, CMAs and notices, contracts, ISAs, MOUs, and other required documentation and restricting unauthorized processing through policies and access controls.

Note: Every information collection is unique; when questions arise needing consultation, contact **Privacy* for policy questions and **Privacy Review* for PCLIA-specific questions.

- (5) To meet this control, you must follow the policies in this IRM on the authority to process personally identifiable information control, including:

IRM	Title
IRM 10.5.1.1	Program Scope and Objectives
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data

- (6) Follow the other PGLD and IRS policies that supplement the authority to process personally identifiable information control, including:

IRM	Title
IRM 10.5.2.1.2	Authority

IRM	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.5.1	Program Scope and Objectives
IRM 10.5.6.1.2	Authority
IRM 10.5.6.2	Privacy Act General Provisions
IRM 10.5.6.3	Privacy Act System of Records Notices (SORNs)
IRM 10.5.6.4	Privacy Notices
IRM 10.5.6.5	Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)
IRM 11.3.1.2	Disclosure Code, Authority and Procedure (CAP)
IRM 1.2.1.2.1	Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights
IRM 1.2.1.17.2	Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safeguarding Confidential Tax Information

10.5.1.8.12.2

(05-08-2025)

PT-03 Personally Identifiable Information Processing and Transparency — Personally Identifiable Information Processing Purposes [P] {Hybrid}

- (1) Identify and document the *legitimate IRS purposes, namely tax administration and other authorized purposes* for processing personally identifiable information;
- (2) Describe the purpose(s) in the public privacy notices and policies of the organization;
- (3) Restrict the *processing* of personally identifiable information to only that which is compatible with the identified purpose(s); and
- (4) Monitor changes in processing personally identifiable information and implement *the Privacy Compliance and Assurance team's processes* to make sure that any changes are made in accordance with *this IRM and the IRS Privacy Principles*. [NIST SP 800-53]
- (5) The IRS requires processing PII only for identified authorized purposes. [Purpose Limitation]
- (6) **Implementation guidance:** The IRS implements this control by requiring that personnel consult with PGLD to make sure any new purposes that arise from changes in processing are compatible with the purpose for which the IRS collected the information. If the new purpose is not compatible, consult with PGLD to implement approaches following defined requirements to allow for the new processing, if proper. Approaches might include obtaining consent from individuals, revising SORNs, updating PCLIAs, or other measures to manage privacy risks that arise from changes in PII processing purposes.

Note: This control is a hybrid organization and system-level control. On the system-level, the PCLIA process addresses the control parameters.

- (7) To meet this control, you must follow the policies in this IRM on the personally identifiable information processing purposes control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities

- (8) Follow the other PGLD and IRS policies that supplement the personally identifiable information processing purposes control, including:

IRM	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.6.2	Privacy Act General Provisions
IRM 10.5.6.3	Privacy Act System of Records Notices (SORNs)
IRM 10.5.6.4	Privacy Notices
IRM 10.5.6.5	Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)
IRM 11.3.1.2	Disclosure Code, Authority and Procedure (CAP)
IRM 1.2.1.2.1	Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights
IRM 1.2.1.17.2	Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safeguarding Confidential Tax Information

10.5.1.8.12.3
(05-08-2025)

**PT-04 Personally
Identifiable Information
Processing and
Transparency —
Consent [P] {Hybrid}**

- (1) Implement appropriate mechanisms (*ability to provide information voluntarily or opt in*) for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making. [NIST SP 800-53]
- (2) The IRS requires allowing individuals to take part in making decisions about the processing of their information and provide consent as required. [Openness and Consent]
- (3) **Implementation guidance:** The IRS implements this control by:
 - a. **Organization-level:** Implied consent. The IRS tax administration system and employment process is based on voluntary compliance where taxpayers and personnel have implied consent by providing their information.
 - b. **System-level:** Opt-in consent. For a system that interacts with the public, the online notices require the individual to opt in (voluntarily providing information or giving consent) to access the system.
- (4) To meet this control, you must follow the policies in this IRM on the consent control, including:

IRM	Title
IRM 10.5.1.3.2.4	Openness and Consent

IRM	Title
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices

- (5) Follow the other PGLD and IRS policies that supplement the consent control, including:

IRM	Title
IRM 10.5.2.2.5.1.4	External Surveys
IRM 10.5.6.4	Privacy Notices
IRM 10.5.6.5	Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)

10.5.1.8.12.4
(05-08-2025)

PT-05 Personally Identifiable Information Processing and Transparency — Privacy Notice [P] {Hybrid}

- (1) Provide notice to individuals about the processing of personally identifiable information that:
 - a. Is available to individuals upon first interacting with an organization, and subsequently at *every major entry point to all IRS public-facing websites and digital services, as well as on any page collecting PII from the public.* [OMB M-23-22, OMB M-03-22]
 - b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language (an overview of IRS privacy practices);
 - c. Identifies the authority that authorizes the processing of personally identifiable information;
 - d. Identifies the purposes for which personally identifiable information is to be processed; and
 - e. Includes *a unique online Privacy Act statement when a system-level website or digital service collects different information from what the IRS.gov privacy policy says.* [OMB M-23-22, OMB M-03-22]

[NIST SP 800-53]
- (2) The IRS requires informing members of the public of our privacy practices and with useful information they would need to make an informed decision about whether and how to interact with the IRS online. [Openness and Consent]
- (3) **Implementation guidance:** The IRS implements this control for an agency privacy policy notice by publishing our privacy policies on *IRS.gov Privacy Policy (external)* and on public-facing system-level websites and digital services with the required elements to individuals before collecting or processing information. This control applies to public-facing (not internal) websites and digital services. Review IRM 10.5.1.8.12.5, PT-05(2) Personally Identifiable Information Processing and Transparency — Privacy Notice - Privacy Act Statements [P] {Hybrid}, for Privacy Act requirements for both internal and public-facing digital services.
 - a. **Organization-level:** Review IRM 10.5.1.6.16.1, IRS.gov Privacy Policy Notice.
 - b. **System-level:** Review IRM 10.5.1.6.16.2, Online Data Collection Privacy Act Statement.

- (4) To meet this control, you must follow the policies in this IRM on the privacy notice control, including:

IRM	Title
IRM 10.5.1.3.2.4	Openness and Consent
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices

- (5) Follow the other PGLD and IRS policies that supplement the privacy notice control, including:

IRM	Title
IRM 10.5.6.4	Privacy Notices
IRM 10.5.6.4.2	Notice to Individuals Asked to Supply Information (Privacy Act Notice)
IRM 10.5.6.4.6	Online Privacy Policy Notices

10.5.1.8.12.5
(05-08-2025)

PT-05(2) Personally Identifiable Information Processing and Transparency — Privacy Notice - Privacy Act Statements [P] {Hybrid}

- (1) Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals. [NIST SP 800-53]
- (2) The IRS requires following the Privacy Act and informing individuals about how we process their PII. [Openness and Consent]
- (3) **Implementation guidance:** The IRS implements this control by providing Privacy Act statements with the required elements to individuals before collecting information in both paper and digital formats.
 - a. **Paper forms:** Review IRM 10.5.6.4.2, Notice to Individuals Asked to Supply Information (Privacy Act Notice), and IRM 10.5.6.4.4, The Umbrella Approach for Tax Returns.
 - b. **Public-facing websites and digital services:** Review IRM 10.5.1.6.16.2, Online Data Collection Privacy Act Statement.
 - c. **Internal-facing websites and digital services:** Review IRM 10.5.1.6.16.4, Internal Websites and Digital Services Privacy Policy and Privacy Act Statement.
- (4) To meet this control, you must follow the policies in this IRM on the Privacy Act statements control, including:

IRM	Title
IRM 10.5.1.3.2.4	Openness and Consent
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices

- (5) Follow the other PGLD and IRS policies that supplement the Privacy Act statement control, including:

IRM	Title
IRM 10.5.6.4	Privacy Notices
IRM 10.5.6.4.2	Notice to Individuals Asked to Supply Information (Privacy Act Notice)
IRM 10.5.6.4.6	Online Privacy Policy Notices

10.5.1.8.12.6

(05-08-2025)

**PT-06 Personally
Identifiable Information
Processing and
Transparency — System
of Records Notice [P]
{Org}**

- (1) For systems that process information that will be maintained in a Privacy Act system of records:
 - a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;
 - b. Publish system of records notices in the Federal Register; and
 - c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

[NIST SP 800-53]
- (2) The IRS requires publishing public-facing notice of the categories, authorities, purposes, and routine uses of the PII that the IRS collects. [Openness and Consent]
- (3) **Implementation guidance:** The IRS implements this control by the publication and updating of SORNs following the *internal SORN SOP (doc)*.
- (4) To meet this control, you must follow the policies in this IRM on the system of records notice control, including:

IRM	Title
IRM 10.5.1.2.7	Privacy Act Information
IRM 10.5.1.3.2.4	Openness and Consent
IRM 10.5.1.6.1.2	Limiting Sharing of SBU Data
IRM 10.5.1.6.15.4	Privacy Act in Contracts

- (5) Follow the other PGLD and IRS policies that supplement the system of records notice control, including:

IRM or Publication	Title
IRM 10.5.2	PCLIA Roles and Responsibilities
IRM 10.5.6.2.9	OMB Privacy Act Guidance
IRM 10.5.6.3	Privacy Act System of Records Notices (SORNs)
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

IRM or Publication	Title
n/a	<i>internal SORN SOP (doc)</i>

10.5.1.8.12.7

(05-08-2025)

PT-06(1) Personally Identifiable Information Processing and Transparency — System of Records Notice - Routine Uses [P] {Org}

- (1) Review all routine uses published in the system of records notice *on a continuous basis, at a minimum once every 3 years* to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected. [NIST SP 800-53]
- (2) The IRS requires reviewing routine uses as compatible with the purpose for which the IRS originally collected the information. [Purpose Limitation]
- (3) **Implementation guidance:** The IRS implements this control by reviewing PCLIA's and SORNs periodically on their proper cycles to make sure that routine uses continue to be compatible with the purpose for which the IRS collected the information. PGLD documents the process in the *internal SORN SOP (doc)*.
- (4) To meet this control, you must follow the policies in this IRM on the routine uses control, including:

IRM	Title
IRM 10.5.1.3.2.2	Purpose Limitation
IRM 10.5.1.2.7	Privacy Act Information

- (5) Follow the other PGLD and IRS policies that supplement the routine uses control, including:

IRM or Publication	Title
IRM 10.5.6.2.9	OMB Privacy Act Guidance
IRM 10.5.6.3	Privacy Act System of Records Notices (SORNs)
IRM 10.5.6-1	Agency Review Requirements
n/a	<i>internal SORN SOP (doc)</i>

10.5.1.8.12.8

(05-08-2025)

PT-06(2) Personally Identifiable Information Processing and Transparency — System of Records Notice - Exemption Rules [P] {Org}

- (1) Review all Privacy Act exemptions claimed for the system of records *on a continuous basis, at a minimum once every year* to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice. [NIST SP 800-53]
- (2) The IRS requires keeping exemption rules proper and necessary. [Purpose Limitation]
- (3) **Implementation guidance:** The IRS implements this control by reviewing PCLIA's and SORNs periodically to make sure that exemptions remain proper. PGLD documents the process in the *internal SORN SOP (doc)*.

- (4) To meet this control, you must follow the policies in this IRM on the system of records notice control, including:

IRM	Title
IRM 10.5.1.3.2.2	Purpose Limitation
IRM 10.5.1.2.7	Privacy Act Information

- (5) Follow the other PGLD and IRS policies that supplement the exemption rules control, including:

IRM or Publication	Title
IRM 10.5.6.2.9	OMB Privacy Act Guidance
IRM 10.5.6.3	Privacy Act System of Records Notices (SORNs)
IRM 10.5.6-1	Agency Review Requirements
n/a	<i>internal SORN SOP (doc)</i>
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.12.9
(05-08-2025)

**PT-07 Personally
Identifiable Information
Processing and
Transparency —
Specific Categories of
Personally Identifiable
Information [P] {Org}**

- (1) Apply *all relevant IRS privacy policy protections* for specific categories of personally identifiable information. [NIST SP 800-53]
- (2) The IRS requires applying privacy protections to PII categories that are sensitive or raise privacy risks, as required by law and policy. [Confidentiality; Security]
- (3) **Implementation guidance:** The IRS implements this control by addressing different categories of PII based on sensitivity and context. If PII is also a Privacy Act record, apply protections required by the Privacy Act. If PII is also tax information, apply protections required by IRC 6103.
- (4) To meet this control, you must follow the policies in this IRM on the specific categories of personally identifiable information control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data
IRM 10.5.1.6.5	Marking
IRM 10.5.1.7.19	Social Security Number Elimination and Reduction (SSN ER)

- (5) Follow the other PGLD and IRS policies that supplement the specific categories of personally identifiable information control, including:

IRM or Publication	Title
IRM 10.5.2.2.2.1	Civil Liberties
IRM 10.5.5.2	IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program
IRM 10.5.6.4.3	Notice to Individuals Asked to Disclose Their Social Security Number
IRM 10.5.6.5	Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)
IRM 11.3 series	Disclosure of Official Information
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.12.10
(05-08-2025)

PT-07(1) Personally Identifiable Information Processing and Transparency — Specific Categories of Personally Identifiable Information - Social Security Numbers [P] {Hybrid}

- (1) When a system processes Social Security numbers:
- Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;
 - Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose their Social Security number; and
 - Inform any individual who is asked to disclose their Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.
- [NIST SP 800-53]
- (2) The IRS requires protecting social security numbers because they are sensitive or raise privacy risks. [Confidentiality; Security]
- (3) **Implementation guidance:** The IRS implements this control by:
- Eliminating the unnecessary use of SSNs.
 - Not denying any right, benefit, or privilege. This does not apply when the SSN is required by federal statute, as in IRC 6109 and 5 USC.
 - Informing taxpayers and personnel that their SSN is mandatory under tax or employment law, and how we will use it.
- (4) To meet this control, you must follow the policies in this IRM on the social security numbers control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities

IRM	Title
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data
IRM 10.5.1.6.5	Marking
IRM 10.5.1.7.19	Social Security Number Elimination and Reduction (SSN ER)

- (5) Follow the other PGLD and IRS policies that supplement the social security numbers control, including:

IRM 10.5.2.2.2.1	Civil Liberties
IRM 10.5.5.2	IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program
IRM 10.5.6.4.3	Notice to Individuals Asked to Disclose Their Social Security Number
IRM 10.5.6.5	Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.12.11
(05-08-2025)

PT-07(2) Personally Identifiable Information Processing and Transparency — Specific Categories of Personally Identifiable Information - First Amendment Information [P] {Org}

- (1) Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity. [NIST SP 800-53]
- (2) The IRS requires keeping First Amendment information out of records, unless expressly authorized, to help prevent selective treatment of persons based on religion, opinion, or group membership. [Purpose Limitation]
- (3) **Implementation guidance:** The IRS implements this control by following the Privacy Act, IRM 10.5.1.6.14.1, First Amendment, IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections), and by not keeping records of how individuals exercise their First Amendment rights except as specifically authorized.
- (4) To meet this control, you must follow the policies in this IRM on the First Amendment information control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.14.1	First Amendment

- (5) Follow the other PGLD and IRS policies that supplement the First Amendment information control, including:

IRM or Publication	Title
IRM 10.5.2.2.2.1	Civil Liberties
IRM 10.5.6.5	Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.12.12
(05-08-2025)

**PT-08 Personally
Identifiable Information
Processing and
Transparency —
Computer Matching
Agreements [P] {Org}**

- (1) When a system or organization processes information for the purpose of conducting a matching program:

- Obtain approval from the Data Integrity Board to conduct the matching program;
- Develop and enter into a computer matching agreement;
- Publish a matching notice in the Federal Register;
- Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and
- Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

[NIST SP 800-53]

- (2) The IRS requires having a way to identify the source of an adverse action if an individual might be subject to an adverse action due to a matching program. {Openness and Consent}
- (3) **Implementation guidance:** The IRS implements this control by requiring computer matching agreements (CMAs) and Treasury Data Integrity Board approval following IRM 11.3.39, Computer Matching and Privacy Protection Act.
- (4) To meet this control, you must follow the policies in this IRM on the computer matching agreements control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.6.1.2	Limiting Sharing of SBU Data
IRM 10.5.1.7.13	Data Services

- (5) Follow the other PGLD and IRS policies that supplement the computer matching agreements control, including:

IRM	Title
IRM 10.5.6.1	Program Scope and Objectives
IRM 11.3.39	Computer Matching and Privacy Protection Act

10.5.1.8.13
(05-08-2025)

**RA-01 Risk Assessment
— Policy and
Procedures [J] {Org}**

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the risk assessment policy and procedures control. For the full text of the control, refer to IRM 10.8.1.4.16, RA-01 Risk Assessment Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Identify and assess risks throughout the privacy lifecycle.
 - b. Respond to risk.
 - c. Conduct privacy impact assessments.
- (3) In this IRM, follow the PGLD policies on the risk assessment policy and procedures control, including:

IRM	Title
IRM 10.5.1.1.5	Background
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data and PII
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.3	Business PII Risk Assessment (BPRA)
IRM 10.5.1.7.16	Incident Management (IM)

- (4) Follow the other PGLD and IRS policies that supplement the risk assessment policy and procedures control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.2.4	Business PII Risk Assessment (BPRA)
IRM 10.5.4.1	Program Scope and Objectives
IRM 10.5.6-1	Agency Review Requirements
Pub 5499	IRS Privacy Program Plan
Document 13347	Data Breach Response Playbook
Document 13347-A	IRS Data Breach Response Plan

10.5.1.8.13.1
(05-08-2025)

**RA-03 Risk Assessment
— Risk Assessment [J]
{Sys}**

- (1) This is a joint security and privacy control about risk assessment. For the full text of the control, refer to IRM 10.8.1.4.16.2, RA-03 Risk Assessment.
- (2) The IRS requires identifying and mitigating privacy risks throughout the privacy lifecycle. [Accountability; Security]

- (3) **Implementation guidance:** The IRS implements this control by conducting PCLIAAs, BPRAs, and other risk assessment, response, and monitoring activities and sharing results with the CPO.
- (4) To meet this control, you must follow the policies in this IRM on the risk assessment control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data and PII
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.3	Business PII Risk Assessment (BPRA)
IRM 10.5.1.7.16	Incident Management (IM)

- (5) Follow the other PGLD and IRS policies that supplement the risk assessment control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.2.4	Business PII Risk Assessment (BPRA)
IRM 10.5.4.1	Program Scope and Objectives
IRM 10.5.6-1	Agency Review Requirements
Pub 5499	IRS Privacy Program Plan
Document 13347	Data Breach Response Playbook
Document 13347-A	IRS Data Breach Response Plan

10.5.1.8.13.2
(05-08-2025)

**RA-07 Risk Assessment
— Risk Response [J]
{Sys}**

- (1) This is a joint security and privacy control about risk response. For the full text of the control, refer to IRM 10.8.1.4.16.6, RA-07 Risk Response.
- (2) The IRS requires responding properly to risk to help protect privacy. [Accountability; Security]
- (3) **Implementation guidance:** The IRS implements this control by avoiding or mitigating risks with strengthened controls, accepting risk with proper justification or rationale, and documenting actions taken.
- (4) To meet this control, you must follow the policies in this IRM on the risk response control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles

IRM	Title
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data and PII
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.3	Business PII Risk Assessment (BPRA)
IRM 10.5.1.7.16	Incident Management (IM)

- (5) Follow the other PGLD and IRS policies that supplement the risk response control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.2.4	Business PII Risk Assessment (BPRA)
IRM 10.5.4.1	Program Scope and Objectives
IRM 10.5.6-1	Agency Review Requirements
Pub 5499	IRS Privacy Program Plan
Document 13347	Data Breach Response Playbook
Document 13347-A	IRS Data Breach Response Plan

10.5.1.8.13.3
(05-08-2025)

**RA-08 Risk Assessment
— Privacy Impact
Assessments [P]
{Hybrid}**

- (1) Conduct privacy impact assessments for systems, programs, or other activities before:
 - a. Developing or procuring information technology that processes personally identifiable information; and
 - b. Initiating a new collection of personally identifiable information that:
 1. Will be processed using information technology; and
 2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

[NIST SP 800-53]
- (2) The IRS requires reviewing IT systems that process PII for privacy risks following the E-Government Act of 2002. [Accountability]
- (3) **Implementation guidance:** The IRS implements this control by requiring PCLIAs for IT systems that process PII.
- (4) To meet this control, you must follow the policies in this IRM on the privacy impact assessments control, including:

IRM	Title
IRM 10.5.1.2.3	Personally Identifiable Information (PII)
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data and PII
IRM 10.5.1.6.14	Civil Liberties
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)

- (5) Follow the other PGLD and IRS policies that supplement the privacy impact assessments control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.6.3	Privacy Act System of Records Notices (SORNs)
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.14
(05-08-2025)

SA-01 System and Services Acquisition — Policy and Procedures [J] {Org}

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the system and services acquisition control. For the full text of the control, refer to IRM 10.8.1.4.17, SA-01 System and Services Acquisition Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
- Fund and manage contracted information resources with PII.
 - Protect data throughout the privacy lifecycle.
 - Include privacy protections in contracts.
 - Engineer systems with minimal PII necessary.
 - Protect privacy in external system services.
 - Protect privacy in development and testing.
- (3) In this IRM, follow the PGLD policies on the system and services acquisition policy and procedures control, including:

IRM	Title
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Roles and Responsibilities
IRM 10.5.1.6.15	Contracts

- (4) Follow the other PGLD and IRS policies that supplement the system and services acquisition policy and procedures control, including:

IRM or Publication	Title
IRM 1.1.27.1.4	Roles and Responsibilities
IRM 1.1.27.7	Program and Planning Support
Pub 4812	Contractor Security & Privacy Controls
Pub 5499	IRS Privacy Program Plan
n/a	<i>internal IRS Acquisition Policy (IRSAP) site Index C (pdf)</i>

10.5.1.8.14.1
(05-08-2025)

**SA-02 System and
Services Acquisition —
Allocation of Resources
[J] {Org}**

- (1) This is a joint security and privacy control about allocation of resources. For the full text of the control, refer to IRM 10.8.1.4.17.1, SA-02 Allocation of Resources.
- (2) The IRS requires funding and managing contracted information resources properly, especially those that involve PII. [Accountability; Minimizing Collection, Use, Retention, and Disclosure]
- (3) **Implementation guidance:** The IRS implements this control by requiring senior management and executives make sure their programs and policies meet this responsibility.
- (4) To meet this control, you must follow the policies in this IRM on the allocation of resources control, including:

IRM	Title
IRM 10.5.1.1	Program Scope and Objectives
IRM 10.5.1.2.1	Privacy Lifecycle
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Roles and Responsibilities
IRM 10.5.1.5	Privacy Culture
IRM 10.5.1.6	Practical Privacy Policy
IRM 10.5.1.7.11	One Solution Delivery Life Cycle (OneSDLC)

- (5) Follow the other PGLD and IRS policies that supplement the allocation of resources control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 1.15.1.1	Program Scope and Objectives
IRM 1.15.2.5	Stages of the Records Life Cycle
IRM 1.1.27.1.4	Roles and Responsibilities
IRM 1.1.27.7	Program and Planning Support

IRM or Publication	Title
Pub 5499	IRS Privacy Program Plan

10.5.1.8.14.2
(05-08-2025)

**SA-03 System and
Services Acquisition —
System Development
Life Cycle [J] {Sys}**

- (1) This is a joint security and privacy control about system development life cycle. For the full text of the control, refer to IRM 10.8.1.4.17.2, SA-03 System Development Life Cycle.
- (2) The IRS requires protecting sensitive data across different life cycle stages, including the system development life cycle (SDLC) and the broader privacy lifecycle because it can be vulnerable. [Accountability; Minimizing Collection, Use, Retention, and Disclosure]
- (3) **Implementation guidance:** The IRS implements this control by requiring that IRS personnel must protect SBU data (including PII and tax information) throughout the privacy lifecycle, from receipt to disposal, which includes the SDLC process.
- (4) To meet this control, you must follow the policies in this IRM on the system development life cycle control, including:

IRM	Title
IRM 10.5.1.1	Program Scope and Objectives
IRM 10.5.1.2.1	Privacy Lifecycle
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.5	Privacy Culture
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data
IRM 10.5.1.6.15	Contracts
IRM 10.5.1.7.11	One Solution Delivery Life Cycle (OneSDLC)

- (5) Follow the other PGLD and IRS policies that supplement the system development life cycle control, including:

IRM	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.6.5.5.2	Relevant and Necessary Guidelines
IRM 1.15.1.1	Program Scope and Objectives
IRM 1.15.2.5	Stages of the Records Life Cycle
Pub 5499	IRS Privacy Program Plan
IRM 1.2.1.2.1	Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights

IRM	Title
IRM 1.2.1.17.2	Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safe-guarding Confidential Tax Information

10.5.1.8.14.3
(05-08-2025)

**SA-04 System and
Services Acquisition —
Acquisition Process [J]
{Sys}**

- (1) This is a joint security and privacy control about acquisition process. For the full text of the control, refer to IRM 10.8.1.4.17.3 , SA-04 Acquisition Process.
- (2) The IRS requires including privacy protections in contracts by following IRM 10.5.1.6.15, Contracts. This means including all privacy requirements language in all contracts, with few approved exceptions. [Accountability]
- (3) **Implementation guidance:** The IRS implements this control by requiring that contractors, subcontractors, and external partners protect all SBU data (including PII and tax information). This means all IRS acquisitions and agreements must include language holding contractors, subcontractors, and other service providers accountable for following federal and IRS privacy policies and procedures. Examples of such policies include privacy requirements language in contracts, PCLIA's for contracted IT, security and privacy controls, and defining contractors as IRS personnel in this IRM with all the same responsibilities for data protection.
- (4) To meet this control, you must follow the policies in this IRM on the acquisition process control, listed in the SA-01 references, IRM 10.5.1.8.14.
- (5) Follow the other PGLD and IRS policies that supplement the acquisition process control in the SA-01 references, IRM 10.5.1.8.14.

10.5.1.8.14.4
(05-08-2025)

**SA-08(33) System and
Services Acquisition —
Security and Privacy
Engineering Principles -
Minimization [P] {Sys}**

- (1) Implement the privacy principle of minimization using *the privacy continuous monitoring process*. [NIST SP 800-53]
- (2) The IRS requires following the “relevant and necessary” requirement of the Privacy Act. [Minimizing Collection, Use, Retention, and Disclosure]
- (3) **Implementation guidance:** The IRS implements this control by collecting only information that is both relevant and necessary to carry out the authorized purpose.
- (4) To meet this control, you must follow the policies in this IRM on the minimization control, including:

IRM	Title
IRM 10.5.1.3.2.3	Minimizing Collection, Use, Retention, and Disclosure
IRM 10.5.1.2.8	Need to Know

- (5) Follow the other PGLD and IRS policies that supplement the minimization control, including:

IRM	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.6.5.5.2	Relevant and Necessary Guidelines
IRM 1.2.1.2.1	Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights
IRM 1.2.1.17.2	Policy Statement 10-2 (New), Privacy First: Protecting Privacy and Safe-guarding Confidential Tax Information

10.5.1.8.14.5
(05-08-2025)

**SA-09 System and
Services Acquisition —
External System
Services [J] {Org}**

- (1) This is a joint security and privacy control about external system services. For the full text of the control, refer to IRM 10.8.1.4.17.8, SA-09 External System Services.
- (2) The IRS requires protecting the IRS's data in external system services. [Security]
- (3) **Implementation guidance:** The IRS implements this control by requiring all IRS external system services contracts and documentation contain proper language holding contractors and other service providers accountable for following federal and IRS privacy policies and procedures, such as privacy requirements language in contracts, PCLIA's for contracted IT, security and privacy controls, and defining contractors as IRS personnel in this IRM with all the same responsibilities for data protection.
- (4) To meet this control, you must follow the policies in this IRMs on the external system services control listed in the SA-01 references, IRM 10.5.1.8.14.
- (5) Follow the other PGLD and IRS policies that supplement the external system services control listed in the SA-01 references, IRM 10.5.1.8.14.

10.5.1.8.14.6
(05-08-2025)

**SA-11 System and
Services Acquisition —
Developer Testing and
Evaluation [J] {Sys}**

- (1) This is a joint security and privacy control about developer testing and evaluation. For the full text of the control, refer to IRM 10.8.1.4.17.10, SA-11 Developer Testing and Evaluation.
- (2) The IRS requires addressing privacy controls and protecting SBU data used in development and testing during the life cycle for acquired systems and services.
- (3) **Implementation guidance:** The IRS implements this control by testing and evaluating of all relevant security and privacy controls and protecting the data used in development and testing.
- (4) To meet this control, you must follow the policies in this IRM on the developer testing and evaluation control, including:

IRM	Title
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.2.1	Privacy Lifecycle
IRM 10.5.1.3.2	IRS Privacy Principles

IRM	Title
IRM 10.5.1.5	Privacy Culture
IRM 10.5.1.6	Practical Privacy Policy
IRM 10.5.1.7.20	SBU Data Use for Non-Production Environments

- (5) Follow the other PGLD and IRS policies that supplement the developer testing and evaluation control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.6.2.9.1	Privacy Act Contract Requirements
IRM 10.5.8.3.2	Requirements for Using SBU Data
IRM 11.3.24.3	Disclosure of Returns and Return Information to Vendors and Expert Services
Pub 5499	IRS Privacy Program Plan
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.15
(05-08-2025)
SC-01 System and Communications Protection — Policy and Procedures [J] {Org}

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the system and communications protection control. For the full text of the control, refer to IRM 10.8.1.4.18, SC-01 System and Communications Protection Policy and Procedures.

Note: This control differs from the NIST baseline where it is a security control, but the IRS will assess it as a joint control.

- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to include privacy in boundary protection.
- (3) In this IRM, follow the PGLD policies on the system and communications protection policy and procedures control, including:

IRM	Title
IRM 10.5.1.1.1	Purpose of the Program
IRM 10.5.1.1.2	Audience
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.5.1	Clean Desk Policy
IRM 10.5.1.6.1	Protecting and Safeguarding SBU Data

IRM	Title
IRM 10.5.1.6.2	Encryption
IRM 10.5.1.6.3	Computers and Mobile Computing Devices
IRM 10.5.1.6.8.2	Emails to Other External Stakeholders
IRM 10.5.1.6.10	Disposition and Destruction
IRM 10.5.1.6.15	Contracts
IRM 10.5.1.6.16	Online Data Collection and Privacy Notices
IRM 10.5.1.6.18	Data on Collaborative Technology and Systems
IRM 10.5.1.7.10	Digital Identity Risk Assessment (DIRA)
IRM 10.5.1.7.12	Governmental Liaison (GL)

- (4) Follow the other PGLD and IRS policies that supplement the system and communications protection policy and procedures control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.4.3	Reporting Losses, Thefts and Disclosures
IRM 10.5.6.2	Privacy Act General Provisions
IRM 11.3.1.1	Program Scope and Objectives
n/a	<i>Internal PCLIA reference guides on the Privacy Impact Assessment Management System site</i>

10.5.1.8.15.1
(05-08-2025)

SC-07(24) Boundary Protection — Personally Identifiable Information [P] {Sys}

- (1) For systems that process personally identifiable information:
 - a. Apply the following processing rules to data elements of personally identifiable information: *all relevant IRS privacy policy protections*;
 - b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;
 - c. Document each processing exception; and
 - d. Review and remove exceptions that are no longer supported.

[NIST SP 800-53]
- (2) The IRS requires processing PII under established privacy requirements only. [Purpose Limitation; Strict Confidentiality; Security]
- (3) **Implementation guidance:** The IRS implements this control by applying rules, monitoring, and documenting exceptions to processing rules.
- (4) To meet this control, you must follow the policies in this IRM on the boundary protection personally identifiable information control listed in the SC-01 references, IRM 10.5.1.8.15.

- (5) Follow the other PGLD and IRS policies that supplement the boundary protection personally identifiable information control listed in the SC-01 references, IRM 10.5.1.8.15.

10.5.1.8.16
(05-08-2025)

SI-01 System and Information Integrity — Policy and Procedures [J] {Org}

- (1) This is a joint security and privacy control requiring that the IRS have policy and procedures about the system and information integrity control. For the full text of the control, refer to IRM 10.8.1.4.19, SI-01 System and Information Integrity Policy and Procedures.
- (2) **Implementation guidance:** The IRS implements this control with policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
- Protect data throughout the privacy lifecycle.
 - Minimize PII throughout the privacy lifecycle, including in testing, training, and research.
 - Enforce a retention period followed by proper disposal.
 - Follow the Privacy Act provisions for amendment and for accurate, relevant, timely, and complete records.
 - De-identify PII in datasets.
- (3) In this IRM, follow the PGLD policies on the system and information integrity policy and procedures control, including:

IRM	Title
IRM 10.5.1.2	Key Privacy Definitions
IRM 10.5.1.3.2	IRS Privacy Principles
IRM 10.5.1.4	IRS-Wide Privacy Roles and Responsibilities
IRM 10.5.1.6.1.2	Limiting Sharing of SBU Data
IRM 10.5.1.6.10	Disposition and Destruction
IRM 10.5.1.6.12	Telework
IRM 10.5.1.6.19	Training
IRM 10.5.1.6.20	Smart Devices
IRM 10.5.1.7.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.1.7.8	Records and Information Management (RIM)

- (4) Follow the other PGLD and IRS policies that supplement the system and information integrity policy and procedures control, including:

IRM or Publication	Title
IRM 10.5.2.2	Privacy and Civil Liberties Impact Assessment (PCLIA)
IRM 10.5.4.4.8	Retention and Disposition
IRM 10.5.6.1.3	Roles and Responsibilities
IRM 10.5.6.2.1	Requirements of the Privacy Act

IRM or Publication	Title
IRM 10.5.6.2.9	OMB Privacy Act Guidance
IRM 10.5.6.5.6	Privacy Act Requirement to Maintain Accurate, Relevant, Timely, and Complete Records
IRM 10.5.6.6	Privacy Act Requests for Non-Tax Records
IRM 11.3.1.4	Disclosure and Safeguarding of Returns and Return Information
IRM 11.3.1.6	Records Disposition For Disclosure
IRM 11.3.11.13	Disclosure of Statistical Data
IRM 11.3.12.6	Protection of Return Information
IRM 11.3.22.2.1.1	Use of Tax Returns in Training Material
IRM 1.15.3.2	Destroying Records in the Custody of the IRS
IRM 1.15.6	Managing Electronic Records
IRM 1.11.2.5.6	Fictitious Identifying Information
Pub 5499	IRS Privacy Program Plan

- 10.5.1.8.16.1
(05-08-2025)
SI-12 System and Information Integrity — Information Management and Retention [J] {Sys}
- (1) This is a joint security and privacy control about information management and retention. For the full text of the control, refer to IRM 10.8.1.4.19.11, SI-12 Information Management and Retention.
 - (2) The IRS requires protecting and minimizing SBU data across the privacy lifecycle. [Minimizing Collection, Use, Retention, and Disclosure]
 - (3) **Implementation guidance:** The IRS implements this control by protecting and minimizing SBU data across the privacy lifecycle, to include minimizing, keeping safely, and disposing properly.
 - (4) To meet this control, you must follow the policies in this IRM on the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.
 - (5) Follow the other PGLD and IRS policies that supplement the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.
- 10.5.1.8.16.2
(05-08-2025)
SI-12(1) System and Information Integrity — Information Management and Retention - Limit Personally Identifiable Information Elements [P] {Sys}
- (1) Limit personally identifiable information being processed in the information life cycle to the following elements of PII: *Minimum necessary PII identified in the PCLIA*. [NIST SP 800-53]
 - (2) The IRS requires minimizing extraneous PII to decrease risk. [Minimizing Collection, Use, Retention, and Disclosure]
 - (3) **Implementation guidance:** The IRS implements this control by minimizing PII throughout the privacy lifecycle.
 - (4) To meet this control, you must follow the policies in this IRM on the information

management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.

- (5) Follow the other PGLD and IRS policies that supplement the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.

10.5.1.8.16.3
(05-08-2025)

SI-12(2) System and Information Integrity — Information Management and Retention - Minimize Personally Identifiable Information in Testing, Training, and Research [P] {Sys}

- (1) Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: *Where possible, use synthetic, fictitious, or masked data.* [NIST SP 800-53]
- (2) The IRS requires using the SBU Data Use process for non-production environments so that other uses of data outside the production environment do not increase privacy risks. [Minimizing Collection, Use, Retention, and Disclosure; Security]
- (3) **Implementation guidance:** The IRS implements this control by requiring the SBU Data Use process for non-production environments, following the training fictitious data requirements, and the protections of research data.
- (4) To meet this control, you must follow the policies in this IRM on the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.
- (5) Follow the other PGLD and IRS policies that supplement the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.

10.5.1.8.16.4
(05-08-2025)

SI-12(3) System and Information Integrity — Information Management and Retention - Information Disposal [P] {Sys}

- (1) Use the techniques to dispose of, destroy, or erase information following the retention period *outlined in the Disposition and Destruction section of IRM 10.5.1, Privacy Policy.* [NIST SP 800-53]
- (2) The IRS requires disposing PII properly because even older information can be sensitive. [Minimizing Collection, Use, Retention, and Disclosure]
- (3) **Implementation guidance:** The IRS implements this control by enforcing a retention period followed by proper disposal.
- (4) To meet this control, you must follow the policies in this IRM on the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.
- (5) Follow the other PGLD and IRS policies that supplement the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.

10.5.1.8.16.5
(05-08-2025)

SI-18 System and Information Integrity — Personally Identifiable Information Quality Operations [P] {Sys}

- (1) Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle *using the privacy continuous monitoring process;* and
- (2) Correct or delete inaccurate or outdated personally identifiable information. [NIST SP 800-53]
- (3) The IRS requires addressing inaccurate PII that might cause problems for individuals, especially in those business functions where inaccurate information

might result in inappropriate decisions or the denial of benefits and services to individuals. [Data Quality; Verification and Notification; Access, Correction, and Redress]

- (4) **Implementation guidance:** The IRS implements this control by following the Privacy Act provisions for accurate, relevant, timely, and complete records.

Note: IRC 7852(e) prohibits using the Privacy Act amendment provisions to change tax records. Refer to IRM 10.5.6.6.3, Requests for Amendment of Non-Tax Privacy Act Records.

- (5) To meet this control, you must follow the policies in this IRM on the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.
- (6) Follow the other PGLD and IRS policies that supplement the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.

10.5.1.8.16.6
(05-08-2025)

SI-18(4) System and Information Integrity — Personally Identifiable Information Quality Operations - Individual Requests [P] {Sys}

- (1) Correct or delete personally identifiable information upon request by individuals or their designated representatives. [NIST SP 800-53]
- (2) The IRS requires addressing inaccurate PII that might cause problems for individuals, especially in those business functions where inaccurate information might result in inappropriate decisions or the denial of benefits and services to individuals. [Data Quality; Verification and Notification; Access, Correction, and Redress]
- (3) **Implementation guidance:** The IRS implements this control by following the Privacy Act provisions for amendment.

Note: IRC 7852(e) prohibits using the Privacy Act amendment provisions to change tax records. Refer to IRM 10.5.6.6.3, Requests for Amendment of Non-Tax Privacy Act Records.

- (4) To meet this control, you must follow the policies in this IRM on the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.
- (5) Follow the other PGLD and IRS policies that supplement the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.

10.5.1.8.16.7
(05-08-2025)

SI-19 System and Information Integrity — De-Identification [P] {Sys}

- (1) Remove the following elements of personally identifiable information from datasets: *in statistical datasets, any identifier or combination of elements that could re-identify an individual, and in all other datasets, limit to minimum necessary PII identified in the PCLIA*; and
- (2) Evaluate *continuously* for effectiveness of de-identification. [NIST SP 800-53]
- (3) The IRS requires de-identifying because certain elements or combinations of elements can re-identify individuals despite efforts to redact, mask, or truncate information. [Minimizing Collection, Use, Retention, and Disclosure]

- (4) **Implementation guidance:** The IRS implements this control by either removing PII elements described in this control or requiring synthetic data in place of PII and tax information where possible.

Note: Removing identifying information (such as name or TIN) from specific tax records does not remove it from the confidentiality protections of IRC 6103.

- (5) To meet this control, you must follow the policies in this IRM on the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.
- (6) Follow the other PGLD and IRS policies that supplement the information management and retention control, listed in the SI-01 references, IRM 10.5.1.8.16.

This Page Intentionally Left Blank

Exhibit 10.5.1-1 (05-08-2025)
Glossary and Acronyms

Term	Definition or description
AO	Authorizing official.
ATO	Authorization to operate.
Authorization to Operate (ATO)	An authorization to operate (ATO) is a formal declaration by a designated approving authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to IRS operations. The ATO is signed after a certification agent (CA) certifies that the system has met and passed all requirements to become operational. Systems continue to operate under the same ATO following the Information System Continuous Monitoring (ISCM) process.
Authorizing Official (AO)	The authorizing official (AO) is a federal employee who is an executive or other senior official with the authority to formally assume responsibility of the operation of an information system and the information contained there, at an acceptable level of risk. (Refer to IRM 10.8.2.3.1.7, Authorizing Official (AO), for more information.)
biometric technology	Biometric technology is a combination of using sensitive personal information with automated analysis, often performed by artificial intelligence processing
BYOD	Bring Your Own Device. A program that enables employees to use their personal handheld devices to access IRS applications and data available before only with government-issued equipment.
civil liberties	The basic rights guaranteed to individual citizens by law.
CMA	Computer matching agreements. Refer to IRM 11.3.39, Computer Matching and Privacy Protection Act, for more information.
CNSI	Classified National Security Information
consent	Consent can be explicit (verbal or by other action) or implied (by continuing or inaction).

Exhibit 10.5.1-1 (Cont. 1) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
controls	From NIST SP 800-53 Rev 5, Section 2.1: Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. Controls are selected and implemented by the organization to satisfy the system requirements. Controls can include administrative, technical, and physical aspects.
COR	Contracting officer's representative
CPO	Chief Privacy Officer
controlled areas	Refer to IRM 10.2.14.3.5, Security Areas.
CSP	Cloud service provider.
Data Owner	Review Information Owner.
DIRA	Digital Identity Risk Assessment.
employee information	All employee information covered by the Privacy Act. Examples include personnel, payroll, job applications, disciplinary actions, performance appraisals, drug tests, health exams, and evaluation data. Most employee information falls under the SBU data category called PII or Privacy information.
ELC	Enterprise Life Cycle; replaced by One Solution Delivery Life Cycle (OneSDLC).
electronic media	Electronic media are electronic copy or devices with bits and bytes such as hard drives, random access memory (RAM), read-only memory (ROM), disks, flash memory, memory devices, phones, mobile computing devices, networking devices, office equipment, and many other types listed in Appendix A of NIST Special Publication 800-88, Guidelines for Media Sanitization.
employees	IRS employees, which includes: <ol style="list-style-type: none"> 1. Employees 2. Seasonal or temporary employees 3. Interns 4. Detailees
EP	Employee Protection, within PGLD's Privacy Policy and Compliance (PPC).

Exhibit 10.5.1-1 (Cont. 2) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
Federal tax information (FTI)	<p>Any return or return information as defined in IRC 6103(b). This includes any information obtained, received, or generated by IRS or any Treasury component with respect to determining liability, potential liability, or amount of liability under the IRC.</p> <p>FTI falls under the SBU data category called tax information or Tax. This IRM uses the term tax information to encompass all kinds of tax data.</p>
FedRAMP	Federal Risk and Authorization Management Program.
fictionalized data	Fictional examples of similar situations with neither the identity of the taxpayer nor any information that could be considered attributable to a taxpayer. Such examples would not require any designation as sensitive.
FIPS	Federal Information Processing Standards.
FISMA	Federal Information Security Modernization Act of 2014.
FTI	Federal tax information.
GL	Governmental Liaison.
GRS	General Records Schedules -Document 12829.
hardcopy	Hardcopy media are physical representations of information, most often associated with paper printouts. Printer and facsimile ribbons, drums, and platens are all examples of hardcopy media. The supplies associated with producing paper printouts are often the most uncontrolled. Hard copy materials that include sensitive data that leave an organization without effective sanitization expose a significant vulnerability to “dumpster divers” and over-curious employees, risking unwanted information disclosures. [NIST Special Publication 800-88, Guidelines for Media Sanitization]

Exhibit 10.5.1-1 (Cont. 3) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
high security items	<p>High security items are original or certified paper documents with SBU data (including PII and tax information), typically received and processed in IRS office controlled or limited areas, that management must not allow personnel to remove from the facility.</p> <p>Note: These are “highly sensitive documents” in IRM 6.800.2, IRS Telework Program. Refer to IRM 10.2.14.3, Protecting Assets.</p> <p>Exception: This policy does not apply to field employees whose positions allow them to have such documents in a field environment (such as Criminal Investigation Special Agents and field compliance Revenue Agents and Revenue Officers). Those positions have more controls and requirements to protect and to process such documents promptly (for example, refer to IRM Parts 5 and 9). For more information about field work, review IRM 10.5.1.6.9.1, Field and Travel, and IRM 10.5.1.6.9, Other Forms of Transmission.</p>
IAD	IRS Agreement Database.
IA	Identity Assurance, within PGLD.
IM	Incident Management, within PGLD’s PPC.
Information Owner (IO)	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information systems vulnerability information	Related to information that if not protected, could result in adverse effects to information systems. Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
IO	Information Owner.

Exhibit 10.5.1-1 (Cont. 4) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
IoT	<p>Internet of Things.</p> <ul style="list-style-type: none">• IoT involves sensing, computing, communication, and actuation. [NIST SP 800-183]• The Internet of Things (IoT) is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. IoT devices are an outcome of combining the worlds of information technology (IT) and operational technology (OT). Many IoT devices are the result of the convergence of cloud computing, mobile computing, embedded systems, big data, low-price hardware, and other technological advances. IoT devices can provide computing functionality, data storage, and network connectivity for equipment that previously lacked them, enabling new efficiencies and technological capabilities for the equipment, such as remote access for monitoring, configuration, and troubleshooting. IoT can also add the abilities to analyze data about the physical world and use the results to better inform decision making, alter the physical environment, and anticipate future events. [NIST IR 8228]
IPP	Information Protection Projects, under PGLD's IRP.
IRC	Internal Revenue Code.
IRP	Identity and Records Protection, under PGLD.

Exhibit 10.5.1-1 (Cont. 5) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
law enforcement sensitive information	<p>Law enforcement data is often sensitive in nature. This data falls under the SBU data category called Law Enforcement, which includes the subcategories:</p> <ul style="list-style-type: none"> • Accident Investigation • Campaign Funds • Committed Person • Communications • Controlled Substances • Criminal History Records Information • DNA • General Law Enforcement • Informant • Investigation • Juvenile • Law Enforcement Financial Records • National Security Letter • Pen Register or Trap & Trace • Reward • Sex Crime Victim • Terrorist Screening • Whistleblower Identity <p>Some of the types of law enforcement data that the IRS might use includes grand jury, informant, and undercover operations information, and procedural guidance.</p>
layered security	<p>Where layered and complementary privacy and security controls are considered sufficient to deter and detect unauthorized entry within the area. Examples include use of perimeter fences, employee and visitor access controls, use of an intrusion detection system, random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during non-working hours. Also sometimes referred to as “security in depth” (refer to IRM 10.2.14.1, Program Scope and Objectives).</p>

Exhibit 10.5.1-1 (Cont. 6) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
legal	<p>Legal data is often sensitive in nature. This data falls under the SBU data category called Legal, which includes the subcategories:</p> <ul style="list-style-type: none"> • Administrative Proceedings • Child Pornography • Child Victim or Witness • Collective Bargaining • Federal Grand Jury • Legal Privilege • Legislative Materials • Pre-sentence Report • Prior Arrest • Protective Order • Victim • Witness Protection <p>Some of the types of legal data that the IRS might use include draft, pre-decisional, and deliberative information.</p>
limited area	Refer to IRM 10.2.14.3.5, Security Areas.
live data	<p>Production data in use.</p> <p>Live means that when changing the data, it changes in production. Authorized personnel may extract the data (such as for testing or development), but then it is <i>no longer live</i>. Live data often includes SBU data.</p>
MCD	Major change determination.
MER	Milestone exit release.
NDA	Non-disclosure agreement.
NIST	National Institute of Standards and Technology.
OFDP	Online Fraud Detection and Prevention, within IT Cybersecurity.
OneSDLC	<p>One Solution Delivery Life Cycle; replaced ELC.</p> <p>Note: The term SDLC on its own usually refers to a system's development. OneSDLC is meant to be more comprehensive solution delivery than traditional system development.</p>
PCA	Privacy Compliance and Assurance.

Exhibit 10.5.1-1 (Cont. 7) (05-08-2025)

Glossary and Acronyms

Term	Definition or description
PCLIA	Privacy and Civil Liberties Impact Assessment; replaced PIA for most privacy assessments. Refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA), for more information.
personally identifiable information (PII)	<p>Per OMB Circular A-130: 'Personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.</p> <p>Because many different kinds of information can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency must perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, recognize that information that is not PII can become PII whenever more information becomes available – in any medium and from any source – that would make it possible to identify an individual.</p> <p>PII as defined here falls under the SBU data category called General Privacy, which is subcategory of the Privacy category. General Privacy refers to personal information, or, in some cases, PII, as defined in OMB M-17-12, or means of identification as defined in 18 USC 1028(d)(7).</p>

Exhibit 10.5.1-1 (Cont. 8) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
personnel	<p>IRS personnel or users, which includes:</p> <ol style="list-style-type: none"> 1. Employees 2. Seasonal or temporary employees 3. Interns 4. Detailees 5. Consultants 6. IRS contractors (including contractors, sub-contractors, non-IRS-procured contractors, vendors, and outsourcing providers) 7. Non-person entity (NPE), such as robotic process automation (RPA), bots, artificial intelligence (AI) workers, or digital assistants. <p>Note: Although these entities are not necessarily capable of following IRS privacy policy, the human parties using them are responsible. These entities must still follow the privacy controls.</p> <p>Subcategory of data in Privacy category.</p>
Personnel record	Any record concerning an individual maintained and used in the personnel management or personnel policy setting process, even if not retrieved by an identifier. [5 CFR 293]
PGLD	Privacy, Governmental Liaison and Disclosure.
PHI	Personal Health Information; falls under the SBU data category called Health Information (part of the Privacy category).
PIA	Privacy Impact Assessment; replaced by PCLIA at IRS for most privacy assessments. Refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA), for more information.
PIAMS	Privacy Impact Assessment Management System.
PII	Personally identifiable information.
POA&M	Plan of action and milestones.
PPC	PGLD's Privacy Policy and Compliance.
PPKM	Privacy Policy and Knowledge Management, under PGLD's PPC.
privacy	Privacy at the IRS shows the joint effort of the IRS, its personnel, and individual taxpayers to protect, control, and exercise rights over the collection, use, retention, dissemination, and disposal of personal information.

Exhibit 10.5.1-1 (Cont. 9) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
Privacy Compliance and Assurance (PCA)	Organization that owns and manages the PCLIA, BPRA, SBU Data Use programs for IRS, under PGLD's PPC.
privacy controls	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. [NIST SP 800-53]
privacy culture	Where all personnel think about privacy before acting. In such an environment or culture, protecting privacy guides the day-to-day practices and routines of everyone.
privacy and information lifecycle	<p>The series of uses and status of information. It includes the creation, collection, receipt, use, processing, maintenance, access, inspection, display, storage, disclosure, dissemination, or disposal of SBU data (including PII and tax information) regardless of format.</p> <p>Note: Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining. [NIST SP 800-53 PT-02]</p> <p>Information life cycle means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion. [OMB A-130]</p> <p>Also described as designation, safeguarding, marking, sharing (accessing and disseminating), destruction, and decontrol.</p>
Privacy Principles	The IRS Privacy Principles describe how the IRS protects an individual's right to privacy. Protecting privacy and safeguarding confidential information is a public trust. To maintain this trust, the IRS and its personnel must follow the privacy principles.
privacy requirements	Mandatory IRS system requirements derived from IRS Privacy Principles and linked to the Privacy Controls, form the basis for privacy protection within the IRS. They mirror the IRS Privacy Principles and provide high-level privacy requirements applicable to the IRS Enterprise Architecture.

Exhibit 10.5.1-1 (Cont. 10) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
processing	Creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal; processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining. [NIST SP 800-53]
QQ	Qualifying Questionnaire (review PCLIA).
RAFT	Risk Acceptance Form and Tool.
RBD	Risk-Based Decision.
RCS	Records Control Schedules -Document 12990
record	Anything you create or receive (in hard copy or electronic format) related to your daily work activities. Refer to the IRM 1.15 series, Records and Information Management, for more information.
requirements	Per NIST SP 800-53, Section 2.1: For federal information security and privacy policies, the term “requirement” is generally used to refer to information security and privacy obligations imposed on organizations. For example, [OMB A-130] imposes information security and privacy requirements that federal agencies must follow when managing information resources. The term “requirement” can also be used in a broader sense to refer to an expression of stakeholder protection needs for a system or organization. Stakeholder protection needs and the corresponding security and privacy requirements may be derived from many sources (such as laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments).
return	Any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity (IRC 6103(b)(1)). Also falls under the SBU data subcategory called federal taxpayer information, which is in the Tax category.

Exhibit 10.5.1-1 (Cont. 11) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
return information	<p>In general, is any information collected or generated by the IRS with regard to any person's liability or possible liability under the IRC. IRC 6103(b)(2)(A) defines return information as very broad.</p> <p>Also falls under the SBU data subcategory called federal taxpayer information, which is in the Tax category.</p>
RIM	Records and Information Management, under PGLD's IRP.
SBU	Sensitive but Unclassified.
SBU data	<p>Any information which, if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations), or the privacy to which individuals are entitled under the Privacy Act (5 USC 552a). [TD P 15-71]</p> <p>SBU data includes:</p> <ul style="list-style-type: none"> Federal tax information (FTI), personally identifiable information (PII), protected health information (PHI), certain procurement information, system vulnerabilities, case selection methodologies, system information, enforcement procedures, investigation information. Live data, which is production data in use. Live means that when changing the data, it changes in production. Authorized personnel may extract the data (such as for testing or development), but then it is no longer live. Live data often includes SBU data. <p>For more information about security protections of SBU data, refer to IRM 10.8.1, Security Policy.</p>
SCIF	Sensitive Compartmented Information Facility (an enclosed area within a building used to process sensitive data).
SDLC	System development life cycle.
sensitive information	SBU data (including PII and tax information); generic plain language term for SBU data for readability.
SLA	Staff-Like Access
SOP	Standard operating procedure

Exhibit 10.5.1-1 (Cont. 12) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
SOR	System of Records
SORN	System of Records Notice
SP	Special Publication (NIST)
SSN ER	Social Security Number Elimination and Reduction.
staff-like access	<p>[From IRM 10.23.2] Staff-like access (SLA) is the authority granted to perform one or more of the following:</p> <ul style="list-style-type: none"> • Enter IRS facilities or space (owned or leased) unescorted (when properly badged). • Possess login credentials to information systems (IRS or vendor-owned systems that store, collect, or process IRS information). • Possess physical or logical access to (including the opportunity to see, read, transcribe, or interpret) SBU data, wherever the location. • Possess physical access to (including the opportunity to see, read, transcribe, or interpret) security items and products (such as items you must store in a locked container, security container, or a secure room, wherever the location. These items include security devices and records, computer equipment, Identification media. Refer to IRM 10.2.14.3, Protecting Assets. • Enter physical areas, wherever the location, that have SBU data (unescorted). <p>SLA is granted to an individual who is not an IRS employee (and includes: contractors and subcontractors, whether procured by IRS or another entity, vendors, delivery persons, experts, consultants, paid or unpaid interns, other federal employees, and cleaning or maintenance employees), and is approved upon required completion of a favorable suitability or fitness determination conducted by IRS Personnel Security.</p>
survey	Any data collection method, including surveys, focus groups, interviews, pilot studies, and field tests. Refer to IRM 10.5.2.2.5.1, Survey PCLIA, for more information.
synthetic data	Data that does not contain SBU data. It imitates data as it appears in an actual taxpayer's file and does not require the submission of an SBU Data Usage and Protection request.

Exhibit 10.5.1-1 (Cont. 13) (05-08-2025)
Glossary and Acronyms

Term	Definition or description
system information	Included in Critical Infrastructure category, also known as information systems vulnerability information. This term includes passwords and vulnerabilities.
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 element assigned to the individual.
System of Records Notice (SORN)	Information which is required to be published in the Federal Register by 5 USC 552a(e)(4). Refer to IRM 10.5.6.3.5, Content of a SORN.
tax information	<p>Any return or return information as defined in IRC 6103(b). This includes any information obtained, received, or generated by IRS or any Treasury component with respect to determining liability, potential liability, or amount of liability under the IRC.</p> <p>For this IRM, the terms tax data and tax information include return and return information as defined in IRC 6103(b).</p> <p>Tax information falls under the SBU data category called FTI or Tax. This IRM uses the term tax information to encompass all kinds of tax data. The Tax category includes:</p> <ul style="list-style-type: none"> • Federal Taxpayer Information. • Tax Convention. • Taxpayer Advocate Information. • Written Determinations.
TIGTA	Treasury Inspector General for Tax Administration.
UNAX	<p>Unauthorized Access; the willful unauthorized access, attempted access or inspection of taxpayer returns or return information.</p> <p>The Taxpayer Browsing Protection Act forbids the willful unauthorized access or inspection of taxpayer records.</p> <ul style="list-style-type: none"> • <i>internal UNAX site</i> • IRM 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements

Exhibit 10.5.1-1 (Cont. 14) (05-08-2025)

Glossary and Acronyms

Term	Definition or description
UUID	Universally Unique Identifier, a unique random number generated for each individual taxpayer in the electronic authentication process (eAuth). It can be PII.

Exhibit 10.5.1-2 (05-08-2025)**References**

This subsection lists tables with many of the primary privacy laws, regulations, guidelines, OMB Memoranda, and other materials that drive the privacy programs. Look to the source for the current published version. You can find some of these on the *Federal Privacy Council's website in the law library section (external)*.

Laws

Law	Citation
Privacy Act of 1974	<i>5 USC 552a (external)</i>
Internal Revenue Code	IRC 6103
Computer Matching and Privacy Protection Act of 1988, which amended the Privacy Act	Pub. L. 100-503
Freedom of Information Act (FOIA)	<i>5 USC 552 (external)</i>
E-Government Act of 2002	Pub.L. 107-347, 116 Stat. 2899, 44 USC 3501 Note, H.R. 2458/S. 803
Federal Information Security Modernization Act of 2014	<i>44 USC 3541 (external)</i>
Protecting Americans from Tax Hikes (PATH) Act of 2015	<i>PL 114-113 (external)(pdf)</i>
Electronic Communications Privacy Act of 1986 (ECPA)	<i>18 USC 2510 (external)</i>
Taxpayer First Act of 2019	<i>133 Stat 981 (external)</i>

Regulations

Regulation	Citation
Personnel records	5 CFR 293
Controlled unclassified information (CUI)	32 CFR 2002
Recording government business	31 CFR 0.215

Executive Orders

Executive Orders (external)

EO	Title
10450	Security Requirements for Government Employment
13556	Controlled Unclassified Information
13636	Improving Critical Infrastructure Cybersecurity
13681	Improving the Security of Consumer Financial Transactions
13960	Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government

Exhibit 10.5.1-2 (Cont. 1) (05-08-2025)**References**

EO	Title
14179	Removing Barriers to American Leadership in Artificial Intelligence

OMB Circulars*OMB Circulars (external)*

OMB Circular	Title
A-11	Preparation, Submission, and Execution of the Budget
A-108	Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
A-130	Managing Information as a Strategic Resource

OMB Memos*OMB Memos (external)*

OMB Memo	Title
M-01-05	Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
M-03-22	OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
M-10-22	Guidance for Online Use of Web Measurement and Customization Technologies
M-10-23	Guidance for Agency Use of Third-Party Websites and Applications
M-12-20	FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. [FAQ 51]
M-14-04	Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. [FAQ 60]
M-16-24	Role and Designation of Senior Agency Officials for Privacy
M-17-09	Management of Federal High Value Assets
M-17-12	Preparing for and Responding to a Breach of Personally Identifiable Information
M-19-17	Enabling Mission Delivery through Improved Identity, Credential, and Access Management
M-20-12	Phase 4 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Program Evaluation Standards and Practices
M-21-04	Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act
M-23-07	Update to Transition to Electronic Records
M-23-22	Delivering a Digital-First Public Experience
M-24-15	Modernizing the Federal Risk and Authorization Management Program (FedRAMP)

Exhibit 10.5.1-2 (Cont. 2) (05-08-2025)**References****Department of the Treasury***Treasury directive publications (external)*

TD P	Title
TD P 15-71	Treasury Security Manual
TD P 25-04	Privacy Act Handbook
TD P 85-01	Treasury Information Technology (IT) Security Program

Related IRS IRMs:

IRM or series	Title
IRM 1.1.27	Privacy, Governmental Liaison and Disclosure (PGLD)
IRM 1.2.1	Service-wide Policies and Authorities, Service-wide Policy Statements
IRM 1.11.2.5.6	Fictitious Identifying Information
IRM 1.15	Records and Information Management
IRM 1.20.2.4	Confidentiality and Disclosure
IRM 1.22	Mail and Transportation Management
IRM 2.31.1	One Solution Delivery Life Cycle Guidance
IRM 4.10	Examination of Returns
IRM 5.1	Field Collecting Procedures
IRM 6.410	Learning and Education
IRM 6.430	Performance Management
IRM 6.800	Employee Benefits
IRM 9.4.6	Surveillance and Non-Consensual Monitoring
IRM 10.2	Physical Security Program
IRM 10.5	Privacy and Information Protection
IRM 10.8	Information Technology (IT) Security
IRM 10.9.1	Classified National Security Information
IRM 10.10	Identity Assurance
IRM 10.23	Personnel Security
IRM 11.3	Disclosure of Official Information
IRM 11.4	Office of Governmental Liaison

Exhibit 10.5.1-2 (Cont. 3) (05-08-2025)**References****NIST**

For the most recent versions, refer to the *NIST website (external)*.

National Institute of Standards and Technology (NIST) Special Publications (SP) (external)

NIST	Title
SP 800-18	Guide for Developing Security Plans for Federal Information Systems
SP 800-28	Guidelines on Active Content and Mobile Code
SP 800-30	Guide for Conducting Risk Assessments
SP 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
SP 800-44	Guidelines on Securing Public Web Servers
SP 800-45	Guidelines on Electronic Mail Security
SP 800-46	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
SP 800-47	Managing the Security of Information Exchanges
SP 800-50	Building a Cybersecurity and Privacy Learning Program
SP 800-53	Security and Privacy Controls for Information Systems and Organizations
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-63 series	Digital Identity Guidelines
SP 800-88	Guidelines for Media Sanitization
SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations
SP 800-163	Vetting the Security of Mobile Applications
NIST SP 800-171	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
SP 800-183	Networks of 'Things'

Federal Information Processing Standards (FIPS) publications (external)

FIPS	Title
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems

Exhibit 10.5.1-2 (Cont. 4) (05-08-2025)**References**

FIPS	Title
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
FIPS 201-3	Personal Identity Verification of Federal Employees and Contractors

Other relevant NIST publications:

NIST	Title
n/a	NIST Risk Management Framework (RMF)
NIST AI 100-1	Artificial Intelligence Risk Management Framework (AI RMF)

IAPP

IAPP (external)