



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.5.1

SEPTEMBER 15, 2023

EFFECTIVE DATE

(09-15-2023)

PURPOSE

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

BACKGROUND

- (1) IRM 10.5.1 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, Program Scope and Objectives: Clarified term processing and cited NIST source.
- (2) IRM 10.5.1.1.1, Purpose of the Program: Updated to reflect current mission statement, cite authorities, link to servicewide policy statement, and identify Bureau Privacy and Civil Liberties Officer (BPCLO).
- (3) IRM 10.5.1.1.2, Audience: Fixed parallelism and explained that human parties behind non-person entities (NPEs) are still required to ensure the NPEs comply with policy.
- (4) IRM 10.5.1.1.3, Policy and Program Owners: Moved BPCLO reference to Purpose of the Program.
- (5) IRM 10.5.1.1.5, Background: Tweaked language about supporting documentation.
- (6) IRM 10.5.1.1.6, Authority: Added authorities that allow IRS to process PII with what restrictions.
- (7) IRM 10.5.1.1.7, Roles and Responsibilities: Added reference to where these are defined, after terminology and concepts have been explained.
- (8) IRM 10.5.1.1.8, Program Management and Review: Reminded business units of their responsibilities and states where PGLD documents program management and review in Pub 5499, IRS Privacy Program Plan.
- (9) IRM 10.5.1.1.9, Program Controls: Explains how the various program controls are owned by business units, PGLD, and the NIST controls for federal IT systems.
- (10) IRM 10.5.1.1.10, Terms and Acronyms: References the extensive Glossary and Acronyms for the convenient compilation of terms.
- (11) IRM 10.5.1.1.11, Related Resources: Links to more detailed listing of references.
- (12) IRM 10.5.1.2.1, Privacy Lifecycle: Explained use of term processing.
- (13) IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data: Clarified language.
- (14) IRM 10.5.1.2.2.1, Examples and Categories of SBU Data: Clarified language.
- (15) IRM 10.5.1.2.3, Personally Identifiable Information (PII): Linked E-Government Act and OMB M-03-22 terminology.
- (16) IRM 10.5.1.2.3.2, Public Record: Clarified tax information requirement.

- (17) IRM 10.5.1.2.3.3, Defining PII versus Sensitive PII: Removed OMB terminology connection and referenced PII definition section because added that connection to PII definition section.
- (18) IRM 10.5.1.2.4, Federal Tax Information (FTI): Clarified terminology.
- (19) IRM 10.5.1.2.7, Privacy Act Information: Clarified that not all PII is Privacy Act information.
- (20) IRM 10.5.1.2.8, Need To Know: Clarified language.
- (21) IRM 10.5.1.2.9, Authentication: Added explanation and references.
- (22) IRM 10.5.1.2.10, Authorization: Added explanation and references.
- (23) IRM 10.5.1.2.11, High Security Items: Clarified language and updated references.
- (24) IRM 10.5.1.3, Key Privacy Concepts: Added link to servicewide policy statement.
- (25) IRM 10.5.1.3.1, Privacy Controls: Added link to IRM 10.8.2 for more about IT roles.
- (26) IRM 10.5.1.3.2, IRS Privacy Principles: Added TBOR language and policy statement link.
- (27) IRM 10.5.1.3.2.1, Accountability: Added plain language description.
- (28) IRM 10.5.1.3.2.2, Purpose Limitation: Added plain language description.
- (29) IRM 10.5.1.3.2.3, Minimizing Collection, Use, Retention, and Disclosure: Added plain language description.
- (30) IRM 10.5.1.3.2.4, Openness and Consent: Added plain language description and clarification about consent.
- (31) IRM 10.5.1.3.2.5, Strict Confidentiality: Added plain language description.
- (32) IRM 10.5.1.3.2.6, Security: Added plain language description.
- (33) IRM 10.5.1.3.2.7, Data Quality: Added plain language description.
- (34) IRM 10.5.1.3.2.8, Verification and Notification: Added plain language description.
- (35) IRM 10.5.1.3.2.9, Access, Correction, and Redress: Added plain language description.
- (36) IRM 10.5.1.3.2.10, Privacy Awareness and Training: Added plain language description.
- (37) IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities: Added reference to role of the Chief Privacy Officer, described in IRM 1.1.27.
- (38) IRM 10.5.1.4.1, Employee/Personnel: Added references to relevant IRS Privacy Principles and clarified terminology.
- (39) IRM 10.5.1.4.2, Management: Clarified language.
- (40) IRM 10.5.1.4.4, System Owners: Added references to OneSDLC process (replacing ELC).
- (41) IRM 10.5.1.4.6, Authorizing Officials: Added references to IRM 10.8.2.
- (42) IRM 10.5.1.4.7, Personnel Engaged in Procurement Activities: Reorganized to highlight the various requirements. Added names of privacy contract clauses.
- (43) IRM 10.5.1.5.1, Clean Desk Policy: Described how policy applies to virtual desktops as well as physical ones.

- (44) IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data: Clarified language.
- (45) IRM 10.5.1.6.1.1, Deciding Risk Levels for SBU Data: Clarified what data is low, moderate, or high confidentiality.
- (46) IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data: Referenced where to find more information about different types of information.
- (47) IRM 10.5.1.6.1.3, Extracting SBU Data: Updated language.
- (48) IRM 10.5.1.6.2, Encryption: Updated references to tools and resources, and combined the subsections External and Internal into this section.
- (49) IRM 10.5.1.6.3, Computers and Mobile Computing Devices: Made active voice.
- (50) IRM 10.5.1.6.5, Marking: Updated policy with how to mark with M365 sensitivity label information.
- (51) IRM 10.5.1.6.6, Storage: Clarified which sections address different types of storage and gave references for external sites, internal collaborative electronic or data sharing, electronic storage, and physical security.
- (52) IRM 10.5.1.6.7, Phone: Clarified language.
- (53) IRM 10.5.1.6.7.1, Cell Phone or Cordless Device: Updated language.
- (54) IRM 10.5.1.6.7.2, Answering Machine or Voicemail: Updated language.
- (55) IRM 10.5.1.6.8, Email: Updated references to tools and resources.
- (56) IRM 10.5.1.6.8.1, Emails to Taxpayers and Representatives: Clarified policy and updated references to approved tools.
- (57) IRM 10.5.1.6.8.2, Emails to Other External Stakeholders: Clarified policy and updated references to approved tools.
- (58) IRM 10.5.1.6.8.3, Emails to IRS Accounts: Added caution about what does not get encrypted.
- (59) IRM 10.5.1.6.8.4, Emails with Personal Accounts: Added content from Interim Guidance Memorandum PGLD-10-1021-0006, Emails with Personal Accounts in Exigent Circumstances, dated 10-19-2021, to clarify policy and add examples.
- (60) IRM 10.5.1.6.8.5, Limited Exceptions to Email SBU Data Encryption: Reorganized section for clarity.
- (61) IRM 10.5.1.6.9.1, Field and Travel: Added note about avoiding smart devices that can record.
- (62) IRM 10.5.1.6.9.2, Mail through USPS: Updated title and added references to telework policy requirements regarding mail.
- (63) IRM 10.5.1.6.9.3, Shipping through Private Delivery Carrier: Updated title and clarified requirements about media encryption, CampusShip usage, the mandatory use and underlying purpose of Form 3210 (or equivalent), a process to track lost or compromised packages, and other shipping requirements.
- (64) IRM 10.5.1.6.9.4, Faxing: Updated language.
- (65) IRM 10.5.1.6.9.5, Printing: Updated references.
- (66) IRM 10.5.1.6.9.6, Text Messaging (Texting): Updated references.

- (67) IRM 10.5.1.6.9.7, Electronic and Online: Changed section name from Electronic to Electronic and Online to address external electronic transmission and online data exchanges.
- (68) IRM 10.5.1.6.10, Disposition and Destruction: Clarified language and updated references.
- (69) IRM 10.5.1.6.10.1, Hardcopy Paper Disposition and Destruction: Updated with plain language.
- (70) IRM 10.5.1.6.10.2, Electronic Disposition and Destruction: Clarified language.
- (71) IRM 10.5.1.6.10.4, Temporary Storage Disposition and Destruction: Clarified language.
- (72) IRM 10.5.1.6.10.5, Records Management Disposition and Destruction: Clarified language.
- (73) IRM 10.5.1.6.10.6, Contractors Disposition and Destruction: Clarified language.
- (74) IRM 10.5.1.6.10.7, Recycling Disposition and Destruction: Clarified language.
- (75) IRM 10.5.1.6.11, Global Positioning Systems (GPS) and Location Services: Clarified language.
- (76) IRM 10.5.1.6.11.1, Global Positioning Systems (GPS): Clarified language.
- (77) IRM 10.5.1.6.11.2, Location Services: Clarified language.
- (78) IRM 10.5.1.6.12, Telework: Moved the information about smart devices to its own section.
- (79) IRM 10.5.1.6.13, Bring Your Own Device (BYOD): Updated links.
- (80) IRM 10.5.1.6.14, Civil Liberties: Updated links.
- (81) IRM 10.5.1.6.14.1, First Amendment: Updated links.
- (82) IRM 10.5.1.6.14.2, Recordings in the Workplace: Reorganized section to give reasons behind security and privacy concerns, then list requirements that allow recording, then steps to follow if recording.
- (83) IRM 10.5.1.6.15, Contractors: Referred to definitions and to requirements in other sections to avoid repetition.
- (84) IRM 10.5.1.6.16, Online Data Collection and Privacy Notices: Added **Collection** to section title, explained more about types of notices, reminded readers about OMB regulations regarding tracking.
- (85) IRM 10.5.1.6.16.1, IRS.gov Privacy Policy Notice: Updated links.
- (86) IRM 10.5.1.6.16.2, Online Data Collection Website or Application Privacy Policy Notice: Added **Online Data Collection** to title, updated template with explanations instead of blanks, and explained when to contact *Privacy.
- (87) IRM 10.5.1.6.16.3, Privacy Departure Notice: Added clarification that not required for links to sites that are not part of an official government domain, although those notices are still recommended. Also added sample departure notice language.
- (88) IRM 10.5.1.6.16.4, Intranet or Non-Publicly Accessible Privacy Policy and Departure Notice: Added **or Non-Publicly Accessible** and **and Departure Notice** to title, explained that this notice is a modified version of the previous one, cited authorities requiring this type of notice, and added a simple example.
- (89) IRM 10.5.1.6.17, Social Media: Updated links.
- (90) IRM 10.5.1.6.18.1, Shared Calendar: Refreshed caution and updated links.

- (91) IRM 10.5.1.6.18.2, Online Meetings: Changed title from **Online Meeting Tools** to reflect that the policy addresses the meetings, updated tools list, added caution about responsibility, focused on key elements (authentication, authorization, need to know), connected clean desk policy, clarified what required before recording (legitimate business need, approval, and consent), gave meeting host responsibilities, and gave tips for data and privacy protection.
- (92) IRM 10.5.1.6.18.3, Shared IRS Storage (OneDrive, SharePoint, Teams, and Other IRS Collaborative Sites): Added content from Interim Guidance Memorandum PGLD-10-1021-0005, Interim Guidance on Shared Storage PIAs, dated 10-18-2021, to replace the SharePoint Privacy Impact Assessment policy and provide updated specific procedures about sensitive but unclassified data (including personally identifiable information and tax information) in collaborative and shared storage locations. Also, merged Shared IRS Storage, SharePoint, Other IRS Collaborative Sites sections and clarified underlying requirements.
- (93) IRM 10.5.1.6.18.4, Cloud Computing: Added references to OneSDLC.
- (94) IRM 10.5.1.6.19, Training: Updated links.
- (95) IRM 10.5.1.6.20, Smart Devices: Added this section (taking most of it from prior Recordings in the Workplace section) and updated examples.
- (96) IRM 10.5.1.6.21, Biometric Technology: Added new section to underscore sensitivity of biometric data and described how to apply IRS Privacy Principles to protect biometric data.
- (97) IRM 10.5.1.7, Privacy-Related Programs: Clarified language.
- (98) IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA): Simplified language and updated links.
- (99) IRM 10.5.1.7.4, Privacy Reporting: Renamed from **Treasury PII Holding Report** and updated section.
- (100) IRM 10.5.1.7.8, Disclosure: Clarified language.
- (101) IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA): Clarified language.
- (102) IRM 10.5.1.7.10, Enterprise Life Cycle (ELC) and One Solution Delivery Life Cycle (OneSDLC): Added OneSDLC, which will eventually replace ELC.
- (103) IRM 10.5.1.7.13.1, Electronic Signature (e-Signature) Program: Added link.
- (104) IRM 10.5.1.7.13.2, Non-Digital Authentication Risk Assessment (NDARA): Renamed section from **Risk Management Authentication in Non-Electronic Channels (Omni Channel Risk Assessment)** and updated links.
- (105) IRM 10.5.1.7.15, Incident Management (IM): Added reminder that IM is not responsible for disciplinary actions.
- (106) IRM 10.5.1.7.17, Safeguards: Updated references and links.
- (107) IRM 10.5.1.7.20, Quick Response (QR) Codes: Clarified language.
- (108) IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls: Clarified when these technical controls apply, reminded readers about definition of processing, added the suffixes and explanations for types of controls (organizational, system, or hybrid), added reminder that the focus is on the data (not the system), restructured each control to change language from **The IRS requires...** to **Implementation guidance: The IRS implements this control by...**, clarified what is meant when a section with subsections is referenced, and added link to the Privacy Controls Checklist.

- (109) IRM 10.5.1.8.1, AC-1 Access Control -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (110) IRM 10.5.1.8.1.1, AC-3(14) Access Control -- Access Enforcement - Individual Access [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (111) IRM 10.5.1.8.2, AT-1 Awareness and Training -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (112) IRM 10.5.1.8.2.1, AT-2 Awareness and Training -- Literacy Training and Awareness [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (113) IRM 10.5.1.8.2.2, AT-3 Awareness and Training -- Role-Based Training [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (114) IRM 10.5.1.8.2.3, AT-3(5) Awareness and Training -- Role-Based Training - Processing Personally Identifiable Information [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (115) IRM 10.5.1.8.2.4, AT-4 Awareness and Training -- Training Records [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (116) IRM 10.5.1.8.3, AU-1 Audit and Accountability -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (117) IRM 10.5.1.8.3.1, AU-2 Audit and Accountability -- Event Logging [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (118) IRM 10.5.1.8.3.2, AU-3(3) Audit and Accountability -- Content of Audit Records - Limit Personally Identifiable Information Elements [P] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (119) IRM 10.5.1.8.3.3, AU-11 Audit and Accountability -- Audit Record Retention [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (120) IRM 10.5.1.8.4, CA-1 Assessment Authorization and Monitoring -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (121) IRM 10.5.1.8.4.1, CA-2 Assessment Authorization and Monitoring -- Control Assessments [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.

- (122) IRM 10.5.1.8.4.2, CA-5 Assessment Authorization and Monitoring -- Plan of Action and Milestones [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (123) IRM 10.5.1.8.4.3, CA-6 Assessment Authorization and Monitoring -- Authorization [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (124) IRM 10.5.1.8.4.4, CA-7 Assessment Authorization and Monitoring -- Continuous Monitoring [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (125) IRM 10.5.1.8.4.5, CA-7(4) Assessment Authorization and Monitoring -- Continuous Monitoring - Risk Monitoring [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (126) IRM 10.5.1.8.5, CM-1 Configuration Management -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (127) IRM 10.5.1.8.5.1, CM-4 Configuration Management -- Impact Analyses [J] {Sys}: Moved under control family. Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (128) IRM 10.5.1.8.6, IR-1 Incident Response -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (129) IRM 10.5.1.8.6.1, IR-2 Incident Response -- Incident Response Training [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (130) IRM 10.5.1.8.6.2, IR-2(3) Incident Response -- Incident Response Training - Breach [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (131) IRM 10.5.1.8.6.3, IR-3 Incident Response -- Incident Response Testing [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (132) IRM 10.5.1.8.6.4, IR-4 Incident Response -- Incident Handling [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (133) IRM 10.5.1.8.6.5, IR-5 Incident Response -- Incident Monitoring [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (134) IRM 10.5.1.8.6.6, IR-6 Incident Response -- Incident Reporting [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.

-
- (135) IRM 10.5.1.8.6.7, IR-7 Incident Response -- Incident Response Assistance [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (136) IRM 10.5.1.8.6.8, IR-8 Incident Response -- Incident Response Plan [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (137) IRM 10.5.1.8.6.9, IR-8(1) Incident Response -- Incident Response Plan - Breaches [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (138) IRM 10.5.1.8.7, MP-1 Media Protection -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (139) IRM 10.5.1.8.7.1, MP-6 Media Protection -- Media Sanitization [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (140) IRM 10.5.1.8.8, PE-1 Physical and Environmental Protection -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (141) IRM 10.5.1.8.8.1, PE-8(3) Physical and Environmental Protection -- Visitor Access Records - Limit Personally Identifiable Information Elements [P] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (142) IRM 10.5.1.8.9, PL-1 Planning -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (143) IRM 10.5.1.8.9.1, PL-2 Planning -- System Security and Privacy Plan [J] {Hybrid}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (144) IRM 10.5.1.8.9.2, PL-4 Planning -- Rules of Behavior [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (145) IRM 10.5.1.8.9.3, PL-4(1) Planning -- Rules of Behavior - Social Media and External Site/Application Usage Restrictions [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (146) IRM 10.5.1.8.9.4, PL-8 Planning -- Security and Privacy Architecture [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (147) IRM 10.5.1.8.9.5, PL-9 Planning -- Central Management [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (148) IRM 10.5.1.8.10.1, PM-3 Program Management -- Information Security and Privacy Resources [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language

from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.

- (149) IRM 10.5.1.8.10.2, PM-4 Program Management -- Plan of Action and Milestones [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (150) IRM 10.5.1.8.10.3, PM-5(1) Program Management -- System Inventory - Inventory of Personally Identifiable Information [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (151) IRM 10.5.1.8.10.4, PM-6 Program Management -- Measures of Performance [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (152) IRM 10.5.1.8.10.5, PM-7 Program Management -- Enterprise Architecture [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (153) IRM 10.5.1.8.10.6, PM-8 Program Management -- Critical Infrastructure Plan [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (154) IRM 10.5.1.8.10.7, PM-9 Program Management -- Risk Management Strategy [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (155) IRM 10.5.1.8.10.8, PM-10 Program Management -- Authorization Process [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (156) IRM 10.5.1.8.10.9, PM-11 Program Management -- Mission and Business Process Definition [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (157) IRM 10.5.1.8.10.10, PM-13 Program Management -- Security and Privacy Workforce [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (158) IRM 10.5.1.8.10.11, PM-14 Program Management -- Testing, Training, and Monitoring [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (159) IRM 10.5.1.8.10.12, PM-15 Program Management -- Security and Privacy Groups and Associations [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (160) IRM 10.5.1.8.10.13, PM-17 Program Management -- Protecting Controlled Unclassified Information on External Systems [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.

-
- (161) IRM 10.5.1.8.10.14, PM-18 Program Management -- Privacy Program Plan [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (162) IRM 10.5.1.8.10.15, PM-19 Program Management -- Privacy Program Leadership Role [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (163) IRM 10.5.1.8.10.16, PM-20 Program Management -- Dissemination of Privacy Program Information [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (164) IRM 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}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (165) IRM 10.5.1.8.10.18, PM-21 Program Management -- Accounting of Disclosures [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (166) IRM 10.5.1.8.10.19, PM-22 Program Management -- Personally Identifiable Information Quality Management [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (167) IRM 10.5.1.8.10.20, PM-23 Program Management -- Data Governance Body [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (168) IRM 10.5.1.8.10.21, PM-24 Program Management -- Data Integrity Board [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (169) IRM 10.5.1.8.10.22, PM-25 Program Management -- Minimization of Personally Identifiable Information Used for Testing, Training, and Research [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (170) IRM 10.5.1.8.10.23, PM-26 Program Management -- Complaint Management [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (171) IRM 10.5.1.8.10.24, PM-27 Program Management -- Privacy Reporting [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (172) IRM 10.5.1.8.10.25, PM-28 Program Management -- Risk Framing [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.
- (173) IRM 10.5.1.8.10.26, PM-31 Program Management -- Continuous Monitoring Strategy [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from "The IRS requires..." to "Implementation guidance: The IRS implements this control by...", and updated links.

-
- (174) IRM 10.5.1.8.11, PS-1 Personnel Security -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (175) IRM 10.5.1.8.11.1, PS-6 Personnel Security -- Access Agreements [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (176) IRM 10.5.1.8.12, PT-1 Personally Identifiable Information Processing and Transparency -- Policy and Procedures [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (177) IRM 10.5.1.8.12.1, PT-2 Personally Identifiable Information Processing and Transparency -- Authority to Process Personally Identifiable Information [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (178) IRM 10.5.1.8.12.2, PT-3 Personally Identifiable Information Processing and Transparency -- Personally Identifiable Information Processing Purposes [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (179) IRM 10.5.1.8.12.3, PT-4 Personally Identifiable Information Processing and Transparency -- Consent [P] {Hybrid}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (180) IRM 10.5.1.8.12.4, PT-5 Personally Identifiable Information Processing and Transparency -- Privacy Notice [P] {Hybrid}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (181) IRM 10.5.1.8.12.5, PT-5(2) Personally Identifiable Information Processing and Transparency -- Privacy Notice - Privacy Act Statements [P] {Hybrid}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (182) IRM 10.5.1.8.12.6, PT-6 Personally Identifiable Information Processing and Transparency -- System of Records Notice [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (183) IRM 10.5.1.8.12.7, PT-6(1) Personally Identifiable Information Processing and Transparency -- System of Records Notice - Routine Uses [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (184) IRM 10.5.1.8.12.8, PT-6(2) Personally Identifiable Information Processing and Transparency -- System of Records Notice - Exemption Rules [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (185) IRM 10.5.1.8.12.9, PT-7 Personally Identifiable Information Processing and Transparency -- Specific Categories of Personally Identifiable Information [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation

guidance: The IRS implements this control by...”, and updated links.

- (186) IRM 10.5.1.8.12.10, PT-7(1) Personally Identifiable Information Processing and Transparency -- Specific Categories of Personally Identifiable Information - Social Security Numbers [P] {Hybrid}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (187) IRM 10.5.1.8.12.11, PT-7(2) Personally Identifiable Information Processing and Transparency -- Specific Categories of Personally Identifiable Information - First Amendment Information [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (188) IRM 10.5.1.8.12.12, PT-8 Personally Identifiable Information Processing and Transparency -- Computer Matching Agreements [P] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (189) IRM 10.5.1.8.13, RA-1 Risk Assessment -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (190) IRM 10.5.1.8.13.1, RA-3 Risk Assessment -- Risk Assessment [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (191) IRM 10.5.1.8.13.2, RA-7 Risk Assessment -- Risk Response [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (192) IRM 10.5.1.8.13.3, RA-8 Risk Assessment -- Privacy Impact Assessments [P] {Hybrid}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (193) IRM 10.5.1.8.14, SA-1 System and Services Acquisition -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (194) IRM 10.5.1.8.14.1, SA-2 System and Services Acquisition -- Allocation of Resources [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (195) IRM 10.5.1.8.14.2, SA-3 System and Services Acquisition -- System Development Life Cycle [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (196) IRM 10.5.1.8.14.3, SA-4 System and Services Acquisition -- Acquisition Process [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (197) IRM 10.5.1.8.14.4, SA-8(33) System and Services Acquisition -- Security and Privacy Engineering Principles - Minimization [P] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.

-
- (198) IRM 10.5.1.8.14.5, SA-9 System and Services Acquisition -- External System Services [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (199) IRM 10.5.1.8.14.6, SA-11 System and Services Acquisition -- Developer Testing and Evaluation [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (200) IRM 10.5.1.8.15, SC-1 System and Communications Protection -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (201) IRM 10.5.1.8.15.1, SC-7(24) Boundary Protection -- Personally Identifiable Information [P] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (202) IRM 10.5.1.8.16, SI-1 System and Information Integrity -- Policy and Procedures [J] {Org}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (203) IRM 10.5.1.8.16.1, SI-12 System and Information Integrity -- Information Management and Retention [J] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (204) IRM 10.5.1.8.16.2, SI-12(1) System and Information Integrity -- Information Management and Retention - Limit Personally Identifiable Information Elements [P] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (205) 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}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (206) IRM 10.5.1.8.16.4, SI-12(3) System and Information Integrity -- Information Management and Retention - Information Disposal [P] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (207) IRM 10.5.1.8.16.5, SI-18 System and Information Integrity -- Personally Identifiable Information Quality Operations [P] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (208) IRM 10.5.1.8.16.6, SI-18(4) System and Information Integrity -- Personally Identifiable Information Quality Operations - Individual Requests [P] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.

- (209) IRM 10.5.1.8.16.7, SI-19 System and Information Integrity -- De-Identification [P] {Sys}: Added the suffix for type of controls (organizational, system, or hybrid), changed language from “The IRS requires...” to “Implementation guidance: The IRS implements this control by...”, and updated links.
- (210) Exhibit 10.5.1-1, Glossary and Acronyms: Updated references in some cases, otherwise:
 - a. Updated terms: Authorizing Official (AO), ELC, system of records.
 - b. Added terms: biometric technology, consent, OneSDLC.
- (211) Exhibit 10.5.1-2, References: Updated references.

EFFECT ON OTHER DOCUMENTS

This version supersedes IRM 10.5.1, dated February 15, 2022. Also, this IRM supports other IRMs in the IRM 10.5 series. This IRM incorporates Interim Guidance Memoranda PGLD-10-1021-0006, Emails with Personal Accounts in Exigent Circumstances, dated 10-19-2021, and PGLD-10-1021-0005, Interim Guidance on Shared Storage PIAs, dated 10-18-2021.

AUDIENCE

IRM 10.5.1 addresses IRS personnel responsible for ensuring adequate privacy and information protection for all Sensitive but Unclassified (SBU) data, including taxpayer and personnel Personally Identifiable Information (PII). This policy applies to all IRS personnel, as defined in the Glossary and Acronyms section.

Peter C. Wade
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/Personnel
 - 10.5.1.4.2 Management
 - 10.5.1.4.3 Senior Management/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 Engaged in Procurement 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
 - 10.5.1.6.2 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 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 Contractors
- 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 Website or Application Privacy Policy Notice
 - 10.5.1.6.16.3 Privacy Departure Notice
 - 10.5.1.6.16.4 Intranet or Non-Publicly Accessible Privacy Policy and Departure Notice
- 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
 - 10.5.1.7 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 Reporting
 - 10.5.1.7.5 Unauthorized Access (UNAX)
 - 10.5.1.7.6 Mandatory Briefings
 - 10.5.1.7.7 Records and Information Management (RIM)
 - 10.5.1.7.8 Disclosure
 - 10.5.1.7.9 Digital Identity Risk Assessment (DIRA)
 - 10.5.1.7.10 Enterprise Life Cycle (ELC) and One Solution Delivery Life Cycle (OneSDLC)
 - 10.5.1.7.11 Governmental Liaison (GL)
 - 10.5.1.7.12 Data Services
 - 10.5.1.7.13 Identity Assurance (IA)
 - 10.5.1.7.13.1 Electronic Signature (e-Signature) Program
 - 10.5.1.7.13.2 Non-Digital Authentication Risk Assessment (NDARA)
 - 10.5.1.7.14 IT Security
 - 10.5.1.7.15 Incident Management (IM)
 - 10.5.1.7.16 Pseudonym
 - 10.5.1.7.17 Safeguards
 - 10.5.1.7.18 Social Security Number Elimination and Reduction (SSN ER)
 - 10.5.1.7.18.1 Acceptable Use of SSNs
 - 10.5.1.7.18.2 SSN Necessary-Use Criteria
 - 10.5.1.7.19 SBU Data Use for Non-Production Environments
 - 10.5.1.7.20 Quick Response (QR) Codes
 - 10.5.1.8 NIST SP 800-53 Security and Privacy Controls
 - 10.5.1.8.1 AC-1 Access Control -- Policy and Procedures [J] {Org}
 - 10.5.1.8.1.1 AC-3(14) Access Control -- Access Enforcement - Individual Access [P] {Org}
 - 10.5.1.8.2 AT-1 Awareness and Training -- Policy and Procedures [J] {Org}
 - 10.5.1.8.2.1 AT-2 Awareness and Training -- Literacy Training and Awareness [J] {Org}
 - 10.5.1.8.2.2 AT-3 Awareness and Training -- Role-Based Training [J] {Org}
 - 10.5.1.8.2.3 AT-3(5) Awareness and Training -- Role-Based Training - Processing Personally Identifiable Information [P] {Org}
 - 10.5.1.8.2.4 AT-4 Awareness and Training -- Training Records [J] {Org}
 - 10.5.1.8.3 AU-1 Audit and Accountability -- Policy and Procedures [J] {Org}
 - 10.5.1.8.3.1 AU-2 Audit and Accountability -- Event Logging [J] {Org}

- 10.5.1.8.3.2 AU-3(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-1 Assessment Authorization and Monitoring -- Policy and Procedures [J] {Org}
 - 10.5.1.8.4.1 CA-2 Assessment Authorization and Monitoring -- Control Assessments [J] {Sys}
 - 10.5.1.8.4.2 CA-5 Assessment Authorization and Monitoring -- Plan of Action and Milestones [J] {Sys}
 - 10.5.1.8.4.3 CA-6 Assessment Authorization and Monitoring -- Authorization [J] {Sys}
 - 10.5.1.8.4.4 CA-7 Assessment Authorization and Monitoring -- Continuous Monitoring [J] {Org}
 - 10.5.1.8.4.5 CA-7(4) Assessment Authorization and Monitoring -- Continuous Monitoring - Risk Monitoring [J] {Org}
- 10.5.1.8.5 CM-1 Configuration Management -- Policy and Procedures [J] {Org}
 - 10.5.1.8.5.1 CM-4 Configuration Management -- Impact Analyses [J] {Sys}
- 10.5.1.8.6 IR-1 Incident Response -- Policy and Procedures [J] {Org}
 - 10.5.1.8.6.1 IR-2 Incident Response -- Incident Response Training [J] {Org}
 - 10.5.1.8.6.2 IR-2(3) Incident Response -- Incident Response Training - Breach [P] {Org}
 - 10.5.1.8.6.3 IR-3 Incident Response -- Incident Response Testing [J] {Org}
 - 10.5.1.8.6.4 IR-4 Incident Response -- Incident Handling [J] {Org}
 - 10.5.1.8.6.5 IR-5 Incident Response -- Incident Monitoring [J] {Org}
 - 10.5.1.8.6.6 IR-6 Incident Response -- Incident Reporting [J] {Org}
 - 10.5.1.8.6.7 IR-7 Incident Response -- Incident Response Assistance [J] {Org}
 - 10.5.1.8.6.8 IR-8 Incident Response -- Incident Response Plan [J] {Org}
 - 10.5.1.8.6.9 IR-8(1) Incident Response -- Incident Response Plan - Breaches [P] {Org}
- 10.5.1.8.7 MP-1 Media Protection -- Policy and Procedures [J] {Org}
 - 10.5.1.8.7.1 MP-6 Media Protection -- Media Sanitization [J] {Sys}
- 10.5.1.8.8 PE-1 Physical and Environmental Protection -- Policy and Procedures [J] {Org}
 - 10.5.1.8.8.1 PE-8(3) Physical and Environmental Protection -- Visitor Access Records - Limit Personally Identifiable Information Elements [P] {Sys}
- 10.5.1.8.9 PL-1 Planning -- Policy and Procedures [J] {Org}
 - 10.5.1.8.9.1 PL-2 Planning -- System Security and Privacy Plan [J] {Hybrid}
 - 10.5.1.8.9.2 PL-4 Planning -- Rules of Behavior [J] {Org}
 - 10.5.1.8.9.3 PL-4(1) Planning -- Rules of Behavior - Social Media and External Site/Application Usage Restrictions [J] {Org}
 - 10.5.1.8.9.4 PL-8 Planning -- Security and Privacy Architecture [J] {Sys}
 - 10.5.1.8.9.5 PL-9 Planning -- Central Management [J] {Org}
- 10.5.1.8.10 PM-1 Program Management
 - 10.5.1.8.10.1 PM-3 Program Management -- Information Security and Privacy Resources [J] {Org}
 - 10.5.1.8.10.2 PM-4 Program Management -- Plan of Action and Milestones [J] {Org}
 - 10.5.1.8.10.3 PM-5(1) Program Management -- System Inventory - Inventory of Personally Identifiable Information [P] {Org}

-
- 10.5.1.8.10.4 PM-6 Program Management -- Measures of Performance [J] {Org}
 - 10.5.1.8.10.5 PM-7 Program Management -- Enterprise Architecture [J] {Org}
 - 10.5.1.8.10.6 PM-8 Program Management -- Critical Infrastructure Plan [J] {Org}
 - 10.5.1.8.10.7 PM-9 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-1 Personnel Security -- Policy and Procedures [J] {Org}
 - 10.5.1.8.11.1 PS-6 Personnel Security -- Access Agreements [J] {Org}
 - 10.5.1.8.12 PT-1 Personally Identifiable Information Processing and Transparency -- Policy and Procedures [P] {Org}
 - 10.5.1.8.12.1 PT-2 Personally Identifiable Information Processing and Transparency -- Authority to Process Personally Identifiable Information [P] {Org}
 - 10.5.1.8.12.2 PT-3 Personally Identifiable Information Processing and Transparency -- Personally Identifiable Information Processing Purposes [P] {Org}
 - 10.5.1.8.12.3 PT-4 Personally Identifiable Information Processing and Transparency -- Consent [P] {Hybrid}
 - 10.5.1.8.12.4 PT-5 Personally Identifiable Information Processing and Transparency -- Privacy Notice [P] {Hybrid}

- hr/>
- 10.5.1.8.12.5 PT-5(2) Personally Identifiable Information Processing and Transparency -- Privacy Notice - Privacy Act Statements [P] {Hybrid}
 - 10.5.1.8.12.6 PT-6 Personally Identifiable Information Processing and Transparency -- System of Records Notice [P] {Org}
 - 10.5.1.8.12.7 PT-6(1) Personally Identifiable Information Processing and Transparency -- System of Records Notice - Routine Uses [P] {Org}
 - 10.5.1.8.12.8 PT-6(2) Personally Identifiable Information Processing and Transparency -- System of Records Notice - Exemption Rules [P] {Org}
 - 10.5.1.8.12.9 PT-7 Personally Identifiable Information Processing and Transparency -- Specific Categories of Personally Identifiable Information [P] {Org}
 - 10.5.1.8.12.10 PT-7(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-7(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-8 Personally Identifiable Information Processing and Transparency -- Computer Matching Agreements [P] {Org}
 - 10.5.1.8.13 RA-1 Risk Assessment -- Policy and Procedures [J] {Org}
 - 10.5.1.8.13.1 RA-3 Risk Assessment -- Risk Assessment [J] {Sys}
 - 10.5.1.8.13.2 RA-7 Risk Assessment -- Risk Response [J] {Sys}
 - 10.5.1.8.13.3 RA-8 Risk Assessment -- Privacy Impact Assessments [P] {Hybrid}
 - 10.5.1.8.14 SA-1 System and Services Acquisition -- Policy and Procedures [J] {Org}
 - 10.5.1.8.14.1 SA-2 System and Services Acquisition -- Allocation of Resources [J] {Org}
 - 10.5.1.8.14.2 SA-3 System and Services Acquisition -- System Development Life Cycle [J] {Sys}
 - 10.5.1.8.14.3 SA-4 System and Services Acquisition -- Acquisition Process [J] {Sys}
 - 10.5.1.8.14.4 SA-8(33) System and Services Acquisition -- Security and Privacy Engineering Principles - Minimization [P] {Sys}
 - 10.5.1.8.14.5 SA-9 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-1 System and Communications Protection -- Policy and Procedures [J] {Org}
 - 10.5.1.8.15.1 SC-7(24) Boundary Protection -- Personally Identifiable Information [P] {Sys}
 - 10.5.1.8.16 SI-1 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
(09-15-2023)
**Program Scope and
Objectives**

- (1) This IRM lays the foundation to:
 - a. Protect the privacy of Sensitive but Unclassified (SBU) data for taxpayers and employees, including personally identifiable information (PII), such as Federal Tax Information (FTI, hereafter called 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 in compliance with the IRS Privacy Principles (cited in IRM 10.5.1.3.2). [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-2]
 - 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 the *Pub 5499, IRS Privacy Program Plan*.
- (2) This IRM covers IRS-wide privacy policy, including but not limited to:
 - 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.

10.5.1.1.1
(09-15-2023)
Purpose of the Program

- (1) The mission of PGLD is to preserve and enhance public confidence by advocating for the appropriate protection, authentication, minimization, retention, and disclosure of sensitive information.
- (2) The privacy and security of taxpayer and employee information is one of the IRS's highest priorities. PGLD administers 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 employee 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 Life Cycle (ELC) and Enterprise Architecture (EA) and One Solution Delivery Life Cycle, (OneSDLC, replacing 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. Comply with privacy requirements and manage privacy risks. [OMB A-130]
 - c. Ensure the protection and proper use of SBU data of the IRS.
 - d. Prevent unauthorized access to SBU data of the IRS.
 - 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) It is acceptable to employ 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, see IRM 10.5.1.3.2, IRS Privacy Principles.

Caution: Policies continue to apply in exigent circumstances. The IRS will post exceptions through *Interim Guidance* 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, Organization and Staffing, Privacy, Governmental Liaison and Disclosure (PGLD), and the *internal PGLD Disclosure and Privacy Knowledge Base*.

10.5.1.1.2 (09-15-2023) **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/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 it is in (such as production, pre-production, and post-production systems).
- (2) For this IRM, the following terms apply.
 - a. IRS personnel or users includes:
 - 1. Employees
 - 2. Seasonal/temporary employees
 - 3. Detailees
 - 4. Interns
 - 5. Consultants

- 6. IRS contractors (including contractors, subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers)
- 7. Non-person entity (NPE) also referred to as robotic process automation (RPA), bots, artificial intelligence (AI) workers, digital assistants etc.

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

- b. Authorized or Unauthorized personnel applies to whether they are authorized or not authorized to perform a particular action.

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]

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. See Exhibit 10.5.1-2, References.
- (2) For more information about PGLD, refer to IRM 1.1.27, Organization and Staffing, 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
(09-15-2023)
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 10.5 series or guidance, IRM 10.5.1 takes precedence, unless the subordinate IRM is more restrictive or otherwise noted.

Note: To deviate from privacy policy, follow the Risk Acceptance Form and Tool (RAFT) process. 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/or acceptance. Submit the RAFT to PPKM for review for compliance with privacy laws and regulations. PPKM will not grant exceptions to bypass laws or mandates. Submit 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 *Office of the Chief Risk Officer*.

10.5.1.1.6
(09-15-2023)

Authority

- (5) This policy assigns responsibilities and lays the foundation necessary to measure privacy progress and compliance.
- (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. See IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For more information about the TBOR, see <https://www.irs.gov/taxpayer-bill-of-rights>. The TBOR requires the IRS to protect taxpayer rights to privacy and confidentiality.
 - (3) In an effort to reference the origin of a privacy policy cited later in this IRM (National Institute of Standards and Technology (NIST), Treasury, etc.), this IRM may reference a requirement's origin in brackets at the end of the guidance, such as [Strict Confidentiality] (IRS Privacy Principles), [AC-1] (NIST SP 800-53 Security and Privacy Controls), or [TD P 85-01] (Treasury Directive Publications). If no specific origin reference appears, multiple origins may apply. Lack of a reference citation does not mean that no origin applies.
 - (4) The primary laws include:
 - Privacy Act (1974).
 - Computer Matching and Privacy Protection Act (1988).
 - Freedom of Information Act (FOIA) (1974).
 - 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 (1997).
 - Federal Information Security Modernization Act of 2014 (FISMA).
 - E-Government Act (2002).
 - Health Insurance Portability and Accountability Act (1996) (HIPAA).
 - (5) The most relevant OMB Circulars and Memos are:
 - 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-14-04 – Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.
 - M-16-24 – Role and Designation of Senior Agency Officials for Privacy.
 - M-17-06 – Policies for Federal Agency Public Websites and Digital Services.

- M-17-12 – Preparing for and Responding to a Breach of Personally Identifiable Information.
- (6) 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).
- (7) The relevant Department of the Treasury directives and publications are:
- 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.
- (8) 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, prior to 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]
- (9) Primary authorities for processing PII include:
- 5 USC, Government Organization and Employees, primarily section 301
 - 18 USC, Crimes and Criminal Procedure, primarily section 1030
 - 26 USC, Internal Revenue Code, primarily sections 6001, 6011, 6012, 6109, 7801
 - 31 USC, Money and Finance, primarily section 330
- (10) For more authorities and links to privacy-related statutes, regulations, guidelines, OMB Memoranda, and other materials relevant to this IRM, see Exhibit 10.5.1-2, References.

10.5.1.1.7
(09-15-2023)

**Roles and
Responsibilities**

- (1) See 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 establishing 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 establishing and documenting the program controls developed to oversee their program as well as ensuring employee compliance with all applicable elements of this IRM.

- (2) For PGLD program controls, the IRS formally documents its privacy program in the *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, see 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) See Exhibit 10.5.1-1, Glossary and Acronyms.

10.5.1.1.11
(09-15-2023)

Related Resources

- (1) See 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
(09-15-2023)

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: Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining. [NIST SP 800-53 PT-2]

- (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
(09-15-2023)

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, but is not limited to:
 - 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, investigation information. See 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 for testing, development, etc., in which case, it is no longer "live." Live data often is SBU data (including PII and tax information); however, tax information stays tax information whether it is *live* in a production environment or is 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 IRS maintains and makes available to taxpayers and other outside parties. IRS personnel must remove access from non-IRS personnel when the need no longer exists. [Strict Confidentiality]
 - a. For more information on encryption and other protections, see IRM 10.5.1.6, Practical Privacy Policy.
 - b. For more information on the need to know, see IRM 10.5.1.2.8, Need To Know.
 - c. Refer to IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, specifically sections titled Access Controls and Least Privilege, for information about limiting access to people who have a need to know the information.
 - d. Refer to IRM 11.3.22, Disclosure of Official Information, Disclosure to Certain Federal Officers and Employees for Purposes of Tax Administration under IRC 6103(h), the Access by IRS Employees Based on Need To Know section.
- (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, 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, see 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, however different protections apply. To determine if publicly available SBU data or SBU data in the public record is still sensitive, see IRM 10.5.1.2.3.2, Public Record.
- (8) Complete a Qualifying Questionnaire for any system using SBU data to determine if it has PII and needs a Privacy and Civil Liberties Impact Assessment (PCLIA). Refer to IRM 10.5.2, Privacy and Information Protection, Privacy Compliance and Assurance (PCA) Program, for more information about PCLIA's.

- (9) For more information on PII, see IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII.

10.5.1.2.2.1
(09-15-2023)

**Examples and
Categories of SBU Data**

- (1) Some examples and categories of IRS SBU data include, but are not limited to:
- a. Personally Identifiable Information (PII) in this IRM refers to Privacy information and its subcategories. These categories include:
 - Contract use.
 - Death records.
 - General privacy.
 - Genetic information.
 - Health information, also known as Protected Health Information (PHI).
 - Inspector General protected.
 - Military personnel records.
 - Personnel records.
 - Student records.
 - b. Tax Information refers to a Tax category that includes:
 - Federal Taxpayer Information (FTI), which includes individual and corporate (or other business) tax return information under IRC 6103.
 - Tax convention.
 - Taxpayer Advocate information.
 - Written determinations.

Note: Tax information is also PII if it identifies an individual.
 - c. Documents marked “Official Use Only” (OUO).
 - d. Certain Procurement information, which can include:
 - General procurement and acquisition (such as contract proposals).
 - Small business research and technology.
 - Source selection.
 - e. Financial information in the Finance category, including:
 - Bank Secrecy Act (31 USC Bank Secrecy Act protected reports filed by financial institutions).
 - Budget.
 - Retirement.
 - Electronic funds transfer.
 - General financial information.
 - International financial institutions.
 - Mergers.
 - Net worth.
 - f. Criminal Investigation and Law Enforcement information, such as:
 - General Law Enforcement (procedures and training materials).
 - Informant (identification, activities, contacts, payments, and correspondence).
 - 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).
 - Law Enforcement Financial Records (and other records obtained via witness consent, subpoena, summons, search warrant, or any other legal process).
 - Pen Register/Trap & Trace.
 - Reward (recipient and payment information).
 - Whistleblower Identity. (Refer to IRC 7623 or the Whistleblower Protec-

tion Act of 1989, Pub.L. 101-12 as amended. For more information, refer to IRM 25.2.1, General Operating Division Guidance for Working Whistle-blower Claims.)

- g. Case selection methodologies including tolerance criteria or general investigation parameters.
- h. Proprietary processes or algorithms used in investigative work or tax processing.
- i. Critical infrastructure category information, which includes:
 - Information system vulnerabilities information (referred to as system information in this IRM), which includes passwords.
 - Physical security information, such as details of facility vulnerabilities (entry codes, badge access, etc.).
 - Emergency management.
- j. Proprietary business information entrusted to the IRS.
- k. Confidential data to be released to the public later.
- l. Legal information, including:
 - Administrative Proceedings.
 - Collective Bargaining.
 - Federal Grand Jury (18 USC Grand Jury information protected by Rule 6(e) of the Federal Rules of Criminal Procedure).
 - Legal Privilege (including draft, pre-decisional, and deliberative information).
 - Legislative Materials (including Congressional or state).
- m. 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).

10.5.1.2.2.2
(12-31-2020)
**Official Use Only and
Limited Official Use**

- (1) By definition, documents designated as **Official Use Only (OUO)** and **Limited Official Use (LOU)** include SBU data.
- (2) For more information, refer to IRM 11.3.12, Disclosure of Official Information, 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
(09-15-2023)
**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, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008, <https://www.gao.gov/products/gao-08-536>]

- (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 whenever more information becomes available — in any medium and from any source — that, when combined with other available information, 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) See IRM 10.5.1.2.3.1, Examples and Categories of PII, for more information.
- (7) Refer to the *internal PGLD Disclosure and Privacy Knowledge Base*.
- (8) Submit a PCLIA for any system using PII. Refer to IRM 10.5.2 for more information about PCLIA's.
- (9) PII in a public record is still PII; however, different protections apply. To determine if publicly available PII or PII in the public record is still sensitive, see IRM 10.5.1.2.3.2, Public Record.
- (10) For more information on PII, see IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII.

10.5.1.2.3.1 (07-08-2021) **Examples and Categories of PII**

- (1) Examples and categories of PII may include, but are not limited to 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:
 - a. Name, such as full name, maiden name, mother's maiden name, alias, or name control (first 4 letters of last name).
 - b. Address information, such as street address or email address.
 - c. A unique set of numbers or characters assigned to a specific individual, such as:
 - 1. Telephone numbers, including mobile, business, and personal numbers.
 - 2. SSN or ITIN, including the last 4 digits.
 - 3. Taxpayer identification number (TIN) that identifies an individual, such as an Employer Identification Number (EIN) for a sole proprietorship or partnership.
 - 4. Document locator number (DLN) to identify an individual's record.

5. Email or Internet Protocol (IP) address.
 6. Driver's license number.
 7. Passport number.
 8. Financial account or credit card number.
 9. Standard Employee Identifier (SEID).
 10. Automated Integrated Fingerprint Identification System (AIFIS) identifier, booking, or detention system number.
 11. Universally Unique Identifier (UUID), a unique random number generated for each individual taxpayer in the electronic authentication process (eAuth).
 12. Any other type of identification number or card, including state ID or Alien Card ID.
- d. Employee and employee information, including personnel files, employment testing materials, medical information, and information concerning reasonable accommodations for disabilities.

Note: For privacy considerations concerning 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, the Health or Safety Disclosure section. For further privacy considerations concerning disability and reasonable accommodation information, refer to IRM 1.20.2, Equity, Diversity and Inclusion, Providing Reasonable Accommodation for Individuals with Disabilities, the Confidentiality and Disclosure section.

- e. Individual tax return information, including Adjusted Gross Income (AGI) or combinations of fields that identify an individual. See IRM 10.5.1.2.4, Federal Tax Information (FTI).
- f. Corporate or other business tax return information that identifies an individual, such as an S-Corporation, partnership, or sole proprietorship.
- g. Personal characteristics and data, including:
1. Date of birth.
 2. Place of birth.
 3. Age.
 4. Height.
 5. Weight.
 6. Gender.
 7. Hair color.
 8. Eye color.
 9. Race.
 10. Ethnicity.
 11. Scars.
 12. Tattoos.
 13. Distinguishing features.
 14. Religious affiliation.
 15. Sexual orientation.
 16. Gang affiliation.
 17. Photographic image (especially of face or other distinguishing characteristic).
 18. Biometric information (such as x-rays, fingerprints, retina scan, voice, facial geometry, DNA).
 19. Behavior patterns.

- h. Asset information, such as Media Access Control (MAC) address, Device ID, or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people.
- i. Descriptions of events or times (information in documents, such as behavior patterns, incident reports, police reports, arrest reports, and medical records).
- j. Descriptions of locations, such as geographic information system (GIS), Global Positioning System (GPS) data, and electronic bracelet monitoring information.
- k. Information identifying personally owned property, such as vehicle registration number or title number and related information.

Exception: “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.

- (2) Information about an individual that is linked or linkable to one of the above.

10.5.1.2.3.2
(09-15-2023)
Public Record

- (1) IRS personnel must protect SBU data regardless of whether the same information is in the public record or publicly available. However, less stringent protections might apply in some situations.
- (2) Generally, personnel must encrypt SBU data (including PII). However, inside the IRS network, encryption is not required if the IRS proactively makes it available to all personnel on internal resource sites (including, but not limited to, Discovery Directory, Outlook [calendar, profile information, and address book], intranet, 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-6(3)_T.124]
- (3) Email addresses, by themselves as the method of the email conveyance, generally do not need encrypting. However, 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. See IRM 10.5.1.6.8, Email, 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.

- (5) No IRC 6103 public records exemption exists. However, the Information Which Has Become Public Record section of IRM 11.3.11, Information Available to the Public, discusses disclosure of matters that have become public records as a result of tax administration, 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-6(3)_T.124]

- (7) The Public Information Listing (PIL) designated by OPM makes certain federal employee information available to the public by FOIA request. For more information, refer to IRM 11.3.13, the Public Information section. [5 CFR 293.311]
- (8) IRS policy also authorizes the withholding of the public information items of employees in cybersecurity designated positions. Cybersecurity designated positions are not identified by a specific GS/IR series or position title.
- (9) Personnel should 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, prior to 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
(09-15-2023)
**Defining PII versus
Sensitive PII**

- (1) Little difference exists between PII and what personnel refer to as “sensitive” PII. For the definition of PII, see IRM 10.5.1.2.3, Personally Identifiable Information (PII).
- (2) The level of risk 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 may still require protection if its context makes it risky. For example, a collection of names:
 - Is not sensitive PII if it is a list, file, query result, etc., of:
 - Attendees at a public meeting.
 - Names out of a public telephone book.
 - FOIA listing of IRS employees in non-protected positions.
 - Is sensitive PII if it is a list, file, query result, etc., of:
 - Individual taxpayers who filed returns.
 - Law enforcement personnel.
 - Employees with poor performance ratings.
- (4) For more information, see IRM 10.5.1.6.1.1, Deciding Risk Levels for SBU Data and PII.

10.5.1.2.4
(09-15-2023)
**Federal Tax Information
(FTI)**

- (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, but is not limited to, 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 it is 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) Submit a Privacy and Civil Liberties Impact Assessment (PCLIA) for any system using SBU data (including PII and tax information). Refer to IRM 10.5.2 for more information about PCLIA's.
- (6) See 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).
- (7) For more information about return information and a definition, refer to IRM 11.3.1, Disclosure of Official Information, Introduction to Disclosure.

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, the Guidance and Requirements section.

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) See 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 U.S. Code Chapter 35 (44 USC 3551-3558); and Privacy Act of 1974, 5 USC 552a.

10.5.1.2.7 (09-15-2023) **Privacy Act Information**

- (1) The Privacy Act of 1974 (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 to prevent misuse of such information.
- (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, but is not limited to, education, financial transactions, medical history, and criminal or employment history and that contains 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. Therefore, 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 the Privacy Act.

Note: Not all PII is Privacy Act information.

- (6) For more information on the conditions of disclosure, refer to IRM 10.5.6, Privacy Act, the Conditions of Disclosure Under the Privacy Act section.

10.5.1.2.8 (09-15-2023) Need To Know

- (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. See examples later in this section for explanations of how need to know applies to duties.

Note: See 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, returning contractors, etc.) 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. If you no longer have a business need to know, you must not access the information. This policy includes, but is not limited to, 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 may 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.

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

- (4) You must ensure your own adherence to 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, efficiently, or appropriately. Necessary for official duties in this context does not mean essential or indispensable, but appropriate 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 ensure they have an appropriate 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, Disclosure of Official Information, Disclosure to Certain Federal Officers and Employees for Purposes of Tax Administration under IRC 6103(h), the Access by IRS Employees section.

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 ensures 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, Information Technology (IT) Security, Policy and Guidance.

10.5.1.2.10
(09-15-2023)
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, the Disclosure Code, Authority, and Procedure (CAP) section.

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]

- (2) 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). Establish authority by a formal request for information processed using established written procedures, or a memorandum of understanding or executed agreement.
- (3) Authorization is required for any person or business conducting IRS business on another person's behalf (such as tax return preparers).
- (4) 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.

10.5.1.2.11
(09-15-2023)
High Security Items

- (1) High security items are original or certified paper documents containing SBU data (including PII and tax information), typically received and processed in IRS office critical or limited areas, that management must not allow to be removed from the facility.

Note: These are "highly sensitive documents" in IRM 6.800.2 Employee Benefits, IRS Telework Program. Refer to IRM 10.2.14, the Protected Items / Information section.

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, see 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, but are not limited to, 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 critical 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 *FAQs: PGLD Telework and Remote Work Guidance* for more information.

- b. The IRS office critical or limited areas include large amounts of information requiring protection or in highly concentrated and easily alterable or destroyable form that is critical and must be protected. Refer to IRM 10.2.14, the Security Areas section.
- c. Do not take high security items to a telework location. See IRM 10.5.1.6.12, Telework. Refer to IRM 6.800.2, the Denial of Telework Agreement Requests section.

Note: You may use electronic or paper copies of high security items, if the originals remain in the office's secured environment.

- (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) Adherence to 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
(09-15-2023)

Privacy Controls

- (1) OMB A-130 mandates federal agencies implement NIST security and privacy controls.
- (2) The IRS formally documents its privacy program in the *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, see IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls.

Note: The section IRM 10.5.1.8 is for technical management officials developing and supporting IT systems, including Management, Senior Management/ Executives, System Owners, System Developers, and Authorizing Officials. For more information about these roles, refer to IRM 10.8.2.

- (4) 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 (i.e., 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
(09-15-2023)
IRS Privacy Principles

- (1) The public trusts the IRS and its personnel to protect taxpayer privacy and safeguard confidential tax information.
- (2) The IRS is dedicated to meeting this expectation. You must act in a way that reflects a commitment to treat individuals fairly, honestly, and respectfully, and always protect their right to privacy. [OMB A-130]
- (3) Protecting taxpayer privacy and safeguarding confidential tax 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.
- (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. See IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For more information about the TBOR, see <https://www.irs.gov/taxpayer-bill-of-rights>. The TBOR requires the IRS to protect taxpayer rights to privacy (with due process) and confidentiality as essential rights that help protect their civil liberties:
<https://www.irs.gov/taxpayer-bill-of-rights>
- (6) IRS Policy Statement 1-1 reflects these principles in the Policy Statements for Organization, Finance and Management Activities section of IRM 1.2.1, Servicewide Policies and Authorities, Servicewide Policy Statements.
- (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.

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 the use of 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
(09-15-2023)

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 it was collected, 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, but is not limited to, 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.

- | | |
|---|--|
| <p>10.5.1.3.2.8
(09-15-2023)
Verification and Notification</p> | <ul style="list-style-type: none"> (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 prior to final action to the greatest extent possible. (2) Privacy is assurance. Verify information and provide individuals with prompt notification before acting. |
| <p>10.5.1.3.2.9
(09-15-2023)
Access, Correction, and Redress</p> | <ul style="list-style-type: none"> (1) Allow individuals to access and correct their PII upon request to the maximum extent allowable. Individuals include, but are not limited to, 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 maximum extent allowable. (2) Privacy is visibility. Allow individuals to access their own information when allowable. Make it right. |
| <p>10.5.1.3.2.10
(09-15-2023)
Privacy Awareness and Training</p> | <ul style="list-style-type: none"> (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. |
| <p>10.5.1.4
(09-15-2023)
IRS-Wide Privacy Roles and Responsibilities</p> | <ul style="list-style-type: none"> (1) The IRS implements privacy roles and responsibilities for personnel following federal laws and privacy guidelines. (2) For the role of the Chief Privacy Officer (CPO), refer to the Roles and Responsibilities section in IRM 1.1.27, Organization and Staffing, Privacy, Governmental Liaison and Disclosure (PGLD). |
| <p>10.5.1.4.1
(09-15-2023)
Employees/Personnel</p> | <ul style="list-style-type: none"> (1) IRS personnel (as defined in IRM 10.5.1.1.2, Audience) must: <ul style="list-style-type: none"> a. Keep informed of and adhere to 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. See the IRS Privacy Principle in IRM 10.5.1.3.2.1, Accountability. b. Limit access to records that include SBU data only to those authorized individuals with a need to know. See 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. c. Use SBU data only for the purposes for which it was collected, unless other purposes are legally mandated or authorized. See the IRS Privacy Principle in IRM 10.5.1.3.2.2, Purpose Limitation. d. 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. See the IRS Privacy Principle in IRM 10.5.1.3.2.2, Purpose Limitation. e. Prevent unnecessary access, inspection, and disclosure of SBU data in information systems, programs, electronic formats, and hardcopy documents by adhering to proper safeguarding measures. See the IRS Privacy Principles in IRM 10.5.1.3.2.5, Strict Confidentiality, and IRM 10.5.1.3.2.6, Security. |

- f. Safeguard IRS information and information systems entrusted to them. See the IRS Privacy Principle in IRM 10.5.1.3.2.6, Security.
- g. Use IRS email accounts for performance of official duties.
- h. Follow existing IT Security Policy and IRS System Security Rules (the IRS *internal Rules of Behavior*) 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, including, but not limited to, the sections AC-20 Use of External Information Systems and Personally-Owned and Other Non-Government Furnished Equipment.
- i. 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. See 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]

- j. 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.
- k. Stay aware of the consequences of UNAX violations, including accessing their 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*.
- l. Report incidents and data breaches immediately upon discovery to:
 - 1. Their manager and
 - 2. The appropriate organizations based on what was lost, stolen, destroyed, or disclosed.

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

- (2) IRS personnel must follow privacy and security responsibilities outlined in IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, and IRM 10.8.2, Information Technology (IT) Security, IT Security Roles and Responsibilities.

10.5.1.4.2
(09-15-2023)
Management

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employee/Personnel, management must also:
 - a. Communicate IRS privacy policies and procedures clearly to all personnel in their 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.

- b. Ensure personnel with authorized access to SBU data receive training to carry out their roles and responsibilities in a manner consistent with IRS privacy policies. [OMB A-130]
- c. Ensure 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.
- d. Prevent UNAX violations proactively in their respective areas. Ensure 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]

- e. Ensure establishment of proper safeguards to prevent unintentional exposure to SSNs in cases where SSN use is determined necessary.
- f. Ensure use of the SEID as the primary employee identifier as an alternative use for SSNs when possible.
- g. Ensure prompt completion of PCLIA's, for which they are the responsible official, and mitigation of any privacy risks discovered.

Note: 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. For more information about the PCLIA process, refer to IRM 10.5.2 and IRM 2.16.1.

- h. Follow IRS records management requirements outlined in the IRM 1.15 series, Records and Information Management.
- i. Ensure all personnel report incidents and data breaches immediately upon discovery to:
 1. Them (as their manager) and
 2. The appropriate organizations based on what was lost, stolen, destroyed, or disclosed.

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

10.5.1.4.3
(12-31-2020)

Senior Management/Executives

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employee/Personnel, and IRM 10.5.1.4.2, Management, senior management/executives must also:
 - a. 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]

- b. 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]
- c. Periodically assess and evaluate privacy awareness activities of their organization to set clear expectations for compliance with all requirements.
- d. Allocate sufficient resources to comply with IRS privacy policies and procedures. [OMB A-130]
- e. Ensure IRS-wide use of alternative unique identifiers for internal and taxpayer systems and programs in place of SSNs when possible.

Note: To deviate from privacy policy, follow the Risk Acceptance Form and Tool (RAFT) process. 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/or acceptance. Submit the RAFT to PPKM for review for compliance with privacy laws and regulations. PPKM will not grant exceptions to bypass laws or mandates. Submit 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 *Office of the Chief Risk Officer*.

10.5.1.4.4
(09-15-2023)
System Owners

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employee/Personnel, IRM 10.5.1.4.2, Management, and IRM 10.5.1.4.3, Senior Management/Executives, IRS IT system owners must:
 - a. 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.
 - b. 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, Lifecycle Management - One Solution Delivery Life Cycle Guidance, or the *OneSDLC site*.
 - c. Follow the NIST SP 800-53 Security and Privacy Controls as cited in IRM 10.5.1.8 and IRM 10.8.1.
 - d. 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.
 - e. 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.
 - f. Ensure that adequate SSN alternatives are employed, as necessary.
 - g. Ensure, to the extent possible, that SBU data used by the IRS to complete business functions is accurate, relevant, timely, and complete.
 - h. Ensure that all new systems, systems under development, or systems undergoing major modifications that contain SBU data have in place a completed and approved PCLIA following federal laws and IRS policy, including the NIST SP 800-53 privacy controls.

Note: The IRS requires PCLIA 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 and IRM 2.16.1.

- i. Work with Privacy Compliance and Assurance (PCA) to review approved PCLIA's to redact SBU data or PII before the PCLIA's are posted to IRS.gov.
- j. Coordinate with the system developer and PCA to ensure documentation of identified privacy risks in their Plans of Action and Milestones (POA&Ms) and prompt resolution.
- k. 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.
- l. Implement safeguards to establish and monitor internal and third-party agreements for the protection of SBU data and to ensure the confidentiality of SBU data.
- m. Ensure 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 prior to being granted access to those systems that include SBU data.
- n. Ensure that IRS personnel who have access to SBU data for testing follow the requirements of IRM 10.5.8, Privacy and Information Protection, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments. For more information, refer to the *internal SBU Data Use Process site*.
- o. Follow IRS records management requirements outlined in the IRM 1.15 series, Records and Information Management.

10.5.1.4.5
(09-15-2023)
System Developers

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employee/Personnel, and IRM 10.5.1.4.2, Management, system developers must:
- a. 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.
 - b. 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, Lifecycle Management - One Solution Delivery Life Cycle Guidance, or the *OneSDLC site*.
 - c. Work with system owners to eliminate the unnecessary accessing, collecting, displaying, sharing, transferring, retaining, and using of SSNs in all IRS systems, especially personnel and tax systems.
 - d. Develop information systems that provide the capability 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.
 - e. Establish, maintain, and test the management, operational, and technical controls to protect SBU data (including PII and tax information).
 - f. Complete system PCLIA's in concert with system owners and following IRS policy, if they are the responsible management official or designees.
- Note:** 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. For more information about the PCLIA process, refer to IRM 10.5.2 and IRM 2.16.1.
- g. Coordinate with the system owners and PCA to resolve identified privacy risks.
 - h. Perform system lifecycle reviews to ensure satisfactory resolution of privacy risks and give the results to the system owners.

10.5.1.4.6
(09-15-2023)
Authorizing Officials

- (1) In addition to the responsibilities in IRM 10.5.1.4.1, Employee/Personnel, and IRM 10.5.1.4.2, Management, the authorizing official (AO) (refer to IRM 10.8.2, the Authorizing Official section) must develop and maintain operational documentation (such as action and implementation plans, standard operating procedures) necessary for implementation of the privacy controls, delineated in the IRM 10.5 series.

Note: To deviate from privacy policy, follow the Risk Acceptance Form and Tool (RAFT) process. 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/or acceptance. Submit the RAFT to PPKM for review for compliance with privacy laws and regulations. PPKM will not grant exceptions to bypass laws or mandates. Submit 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 *Office of the Chief Risk Officer*.

- (2) The AO holds responsibility for implementation of privacy, including documentation and procedures for managing, administering, and monitoring their information systems. For more information about this role, refer to IRM 10.8.2.

10.5.1.4.7
(09-15-2023)
Personnel Engaged in Procurement Activities

- (1) In addition to the Employee/Personnel responsibilities, personnel engaged in procurement-related activities involving SBU data (including PII and tax information) must address these items:

- a. **COR training:** Review and understand the proper privacy procurement-related training and guidance, including the Contracting Officer Representative (COR) Security, Privacy, and Disclosure Awareness Training.

Note: For more information, see IRM 10.5.1.6.15, Contractors, and refer to IRM 11.3.24.

- b. **OneSDLC:** Follow the OneSDLC process. For more information about OneSDLC, refer to IRM 2.31.1, Lifecycle Management - One Solution Delivery Life Cycle Guidance, or the *OneSDLC site*.
- c. **Contract clauses:** Ensure all IRS acquisition, procurement, and contract documents contain proper language holding contractors and other service providers accountable for following federal and IRS privacy policies and procedures. [OMB A-130] For any contract or agreement involving access to SBU data (including PII and tax information), you must insert the necessary contract clauses found on the *IRS Acquisition Policy site*. Look for these clauses:
 - IR1052.204-9000 Submission of Security Forms and Related Materials
 - IR1052.204-9001 Notification of Change in Contractor Personnel Employment Status, Assignment, or Standing
 - IR1052.224-9000 Safeguards Against Unauthorized Disclosure of Sensitive but Unclassified Information
 - IR1052.224-9001 Mandatory IRS Security and Privacy Training for Information Systems, Information Protection and Facilities Physical Access
- d. **Privacy Act (SORN):** Ensure contract work statements 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. Include the Privacy Act authority, use, protec-

tions, and penalties for violations. Refer to IRM 10.5.6, Privacy Act, the Privacy Act Contract Requirements section.

- e. **IRC 6103 (tax information):** If the contract or agreement involves tax information, ensure the contract includes IRC 6103 authority, use, protections, and penalties for violations. Refer to IRM 11.3.24, Disclosures to Contractors, the Requirements section.
- f. **Background investigation:** Support the proper level of contractor background investigation in cooperation with the Office of Contractor Security Management (CSM) and Office of Personnel Security (PS) as described in IRM 10.23.2, Personnel Security – Contractor Investigations. This includes working with PS to assign the correct risk designations (often Moderate for access to SBU data), helping with contractor fingerprinting, and distributing identity cards, if needed. If contractors need re-investigation every five years, the COR must start those. For position risk designations:
 - 1. All contracting actions with SBU data (including PII and tax information), with some exceptions, carry a Moderate impact security level.
 - 2. Contracts with staff-like access to FISMA systems carry a High impact security level.

Note: These are security impact levels, not background investigation levels. Refer to Pub 4812, Contractor Security & Privacy Controls, the Security Categorization section.

Note: Any staff-like access (facilities, systems, or SBU data) requires completion of a favorable suitability/fitness determination (background investigation) conducted by IRS Personnel Security. For more information about staff-like access, refer to IRM 10.23.2.

- g. **Mandatory training:** Ensure contractors take required security, privacy, disclosure, and UNAX training within the required time frames per CSM instructions.

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 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]

- h. **Non-disclosure agreements (NDAs):** Complete Non-Disclosure Agreements (NDAs) within the required time frames per CSM instructions.

Note: All contractors must sign NDAs before given access to SBU data (including PII and tax information).

- i. **Privacy and security controls:** Ensure contractors with access to SBU data follow Pub 4812, Contractor Security & Privacy Controls (which incorporates IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls, and IRM 10.8.1, as well as the relevant 10.8 series IRMs).
- j. **Testing and development environments:** Ensure any contract involving the use of SBU data in testing and development environments follows 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*.
- k. **PCLIA:** Ensure contractors receive and understand the PCLIA when supporting a project with a PCLIA. In some cases, contractors might need to

work with the IRS to complete the required PCLIA. Before “developing or procuring information technology that collects, maintains, or disseminates” SBU data (including PII and tax information), the IRS must complete a PCLIA. [E-Government Act]

Note: 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 and IRM 2.16.1.

- l. **Incident response:** Ensure the contractor understands incident response requirements. All incidents related to IRS processing, information, or information systems must be reported immediately upon discovery to the CO and COR. Report security incidents to Computer Security Incident Response Center (CSIRC) by contacting the CSIRC Support Desk at 240-613-3606. Refer to Pub 4812, the IR-6 Incident Reporting section.
- m. **UNAX:** Report UNAX by a contractor to TIGTA and Procurement.
- n. **Contract closeout:** Collaborate with CSM at contract closeout to revoke system and facilities accesses and to ensure all IRS data is returned or purged as required by the contract.
- o. **FAR compliance:** Ensure compliance with the Federal Acquisition Regulations (FAR). For more information, refer to the FAR site:
<https://www.acquisition.gov/browse/index/far>

[OMB A-130]

- (2) For more information, refer to *internal Contractor Compliance site*.
- (3) Email Privacy Policy for help with these responsibilities at **Privacy*.
- (4) For more information, refer to the *internal Procurement site*.

10.5.1.5 (12-31-2020) **Privacy Culture**

- (1) The IRS requires a privacy culture, wherein 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 (09-15-2023) **Clean Desk Policy**

- (1) The IRS has a clean desk policy. To protect SBU data (including PII and tax information) when it is 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, desk tops, fax/copy machines, conference rooms, and in/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. See 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 and/or when not under the direct control of an authorized IRS employee. For more information, refer to IRM 10.2.14, Methods of Providing Protection, the Containers section.
- (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. 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, the Protected Items / Information section.
 - 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. Forwarded by the business unit to PGLD for approval via email to **Privacy*. Facilities Management and Security Services (FMSS) will conduct the physical onsite reviews, with assistance 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.

Note: 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.

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 should 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 reflects 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 whenever 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 sections 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*.
For help, email **Privacy*.

10.5.1.6.1
(09-15-2023)
**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) The requirements in this section 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.
- (3) 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.
- (4) Take steps to prevent the possibility of such disclosure by non-IRS personnel. Deny unauthorized non-IRS personnel access to other than IRS areas established for serving the public.
- (5) Follow the IRS Clean Desk Policy in IRM 10.5.1.5.1.
- (6) Determine 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.
- (7) 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.
- (8) 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 ensure 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.
- (9) IRS personnel must protect SBU data supporting their mission, operations, and assets. Protection efforts must focus on preventing unauthorized or inadvertent

disclosure and 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/digital assistants, smart devices, Internet of Things (IoT), portable/pocket computers, cameras, and other video imaging recorders, flash drives, multi-functional, and two-way pagers, and wireless devices capable of storing, processing, or transmitting information.

- (10) IRS program managers and contracting officials must also require properly privacy and security contract clauses 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
(09-15-2023)

**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 substantial harm, embarrassment, inconvenience, or unfairness to an individual 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, see 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.
- (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, see 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, Information Technology (IT) Security, Policy and Guidance.

10.5.1.6.1.2
(09-15-2023)

Limiting Sharing of SBU Data

- (1) We must protect all SBU data (including PII and tax information). Limit what SBU we share based on authentication, authorization, and need to know. See IRM 10.5.1.2, Key Privacy Definitions. [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 designated individuals.
- (3) You may reproduce SBU data only to the extent needed to carry out official business. Properly destroy flawed or otherwise unusable reproductions. See the Disposition and Destruction section in IRM 10.5.1.6.10, Disposition and Destruction.
- (4) For tax information, follow extensive Disclosure rules in the IRM 11.3 series, Disclosure of Official Information.
- (5) For Privacy Act information, follow IRM 10.5.6, the Conditions of Disclosure under the Privacy Act section.
- (6) **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.
- (7) The electronic transmission of SBU data (including PII and tax information) requires encryption for security purposes. See IRM 10.5.1.6.2, Encryption, and IRM 10.5.1.6.9.7, Electronic and Online, for more information.
- (8) 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.

Note: Removing identifying information (such as name or TIN) from specific tax records does not remove it from the confidentiality protections of IRC 6103.

- (9) **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. Establish authority by a formal request for information 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/program, such as IRS Agreement Database (IAD). For more information about the IAD, see IRM 10.5.1.7.11, 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, the Privacy Act System of Records Notices (SORNs) section.

- (10) 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.
- a. To do so, submit 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, Privacy Compliance and Assurance (PCA) Program.

10.5.1.6.2
(09-15-2023)
Encryption

- (1) Encryption is a crucial tool in the IRS’s protection of SBU data (including PII and tax information). [OMB A-130, Security]
- (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, but is not limited to, 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, the Media Use section, and *removable media guidance on internal IRS Service Central site*.

- (3) For more details about emailing and encrypting SBU data, see IRM 10.5.1.6.8, Email.

Note: Different policies apply for emails to taxpayers and representatives, other stakeholders, those with IRS accounts, and personal email. For more information and requirements about emailing outside the IRS, see 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; and IRM 10.5.1.6.8.4, Emails with Personal Accounts; and IRM 10.5.1.6.8, Email.

- (4) Instructions for using SecureZip to encrypt attachments also are available on the *internal IRS Service Central site*. See the Virtual Library for more information about encrypting documents, emails, and email attachments on the *internal Encryption site*.
- (5) 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, Information Technology (IT) Security, Policy and Guidance, in the Cryptographic Protection, Access Control, Media Protection, and Physical and Environmental Protection sections.

10.5.1.6.3
(09-15-2023)
**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, smartphone, etc.]). 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 Physical Security Program policies or contractual requirements.
 - b. In addition, 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, smartphone, etc.]) 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.

Note: This policy applies even to personnel who live alone. Always secure equipment.

- (4) For more information about secured wireless access points (wi-fi hotspots), see IRM 10.5.1.6.12, Telework, and refer to IRM 10.8.1, Information Technology (IT) Security Policy and Guidance, the AC-18 Wireless Access section.

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 to your manager and the appropriate organizations based on what was lost or disclosed. [OMB A-130]

- (3) For a brief description of the Incident Management program, see IRM 10.5.1.7.15, Incident Management.
- (4) For more information about how to report an incident, refer to IRM 10.5.4, Privacy and Information Protection, Incident Management Program, or the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.

10.5.1.6.5
(09-15-2023)
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. IRM 11.3.12, Designation of Documents, includes IRS-specific marking requirements. The lack of SBU markings, however, does not relieve the holder from safeguarding responsibilities. Do not remove, mark, and restore unmarked

SBU information already in records storage. However, if you remove unmarked SBU items from storage, you must mark them properly before processing or re-filing.

- (2) Identify and mark SBU data at document creation.
- (3) If you handle unmarked SBU data, consider marking when possible.
- (4) For documents and sites in the M365 environment (such as in email, Word, Excel, and PowerPoint), consider using sensitivity labels. Current simple sensitivity labels include:
 - a. Federal Tax Information (FTI). If your sensitive file has FTI, use the FTI label.
 - b. Personally Identifiable Information (PII). If your sensitive file has PII (but not FTI), use the PII label.
 - c. Sensitive But Unclassified (SBU). If the file has SBU data (but not PII or FTI), then use the SBU label.
 - d. Uncontrolled – not SBU. If your file isn't sensitive, you may use the Uncontrolled - not SBU label.

FTI is the highest sensitivity, while Uncontrolled – not SBU is the lowest. Change your label as needed, justifying the change if you lower the sensitivity. For more information, refer to the *internal Sensitivity Labels site*.

- (5) TD P 15-71 requires that you:
 - a. Prominently mark items that include SBU information at the top/bottom of the front/back cover and each individual page with the marking "SENSITIVE BUT UNCLASSIFIED" or "SBU." Information system prompts may be adjusted to incorporate SBU markings in headers and footers.
 - b. Mark portions, paragraphs, and subject titles that include SBU information with the abbreviation "SBU" to differentiate it from the remaining text. Only when the entire text has SBU information are individual portion markings optional.
 - c. Controlling, decontrolling, or originator information markings are not required.
 - d. When sent outside IRS, except for tax information sent to a taxpayer, documents with SBU data must include a statement alerting the recipient, either in a transmittal letter or directly on the document.

Example: This document belongs to the IRS. Do not release without the express permission of (creating office). Refer requests and inquiries for the document to: (insert name and address of originating office and contact number(s)).

[TD P 15-71]

Note: These marking requirements pre-date IRS implementation of the 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*.

- (6) Protective measures start when we apply markings and end when we cancel such markings or destroy records.

- (7) Although SBU is Treasury's standard for identifying sensitive information, some types of SBU information might be more sensitive than others and call for more safeguarding measures beyond the minimum requirements established 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. IRS and its personnel must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property/equipment as the basis for determining the need for safeguards more than the minimum requirements here.
- (8) A **green** Sensitive But Unclassified (SBU) Cover Sheet, *Other Gov TDF 15-05.11*, must be placed on documents that have SBU material to prevent unauthorized or inadvertent disclosure when SBU information is removed from an authorized storage location and persons without a need-to-know are present or casual observation would reveal SBU information.
 - a. When sending SBU information, 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, see IRM 10.5.1.6.9.7, Electronic and Online.
 - For internal collaborative electronic or online data sharing, see 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 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, the Media Use section, and *removable media guidance on internal IRS Service Central site*.

- (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, Methods of Providing Protection, the Protected Items / Information section.
- (4) For storage of federal records, refer to IRM 1.15 series, Records and Information Management.
- (5) For managers handling employee performance files (EPFs), refer to the sections:
 - Maintaining Tax Return Information in Employee Performance Files section in IRM 11.3.22.

- Employees in Critical Job Elements in IRM 6.430.2, Performance Management, Performance Management Program for Evaluating Bargaining Unit and Non-Bargaining Unit Employees Assigned to Critical Job Elements (CJEs).
- Performance Management Program for Evaluating Managers, Management Officials and Confidential Management/Program Analysts in IRM 6.430.3, Performance Management, Performance Management Program for Evaluating Managers, Management Officials and Confidential Management/Program Analysts.

10.5.1.6.7
(09-15-2023)
Phone

- (1) When communicating SBU data (including PII and tax information) via phone, IRS personnel must:
 - a. Authenticate the individual. See IRM 10.5.1.2.9, Authentication.
 - b. Confirm you're talking to an authorized person before discussing the information. See IRM 10.5.1.2.10, Authorization.
 - c. Inform them you'll be talking about sensitive information.

10.5.1.6.7.1
(09-15-2023)
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. However, use of these devices might raise some vulnerability issues. Refer to IRM 10.8.1, the Telecommunication Devices and the Personally-Owned and Other Non-Government Furnished Equipment sections.
- (2) Whenever 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. Appropriately 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, Classified National Security Information.
- (8) For information about text messaging or texting, see IRM 10.5.1.6.9.6, Text Messaging (Texting).

10.5.1.6.7.2 (09-15-2023)

Answering Machine or Voicemail

- (1) Use the following for answering machine and voicemail guidelines when leaving messages with sensitive information:
- You generally may not leave tax information protected by IRC 6103 on an answering machine or voicemail. However, 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, the fact 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.
 - The following 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.
 - Document the taxpayer's or representative's telephone number, their approval to call that number, and their permission for IRS to leave information on the recording.
 - Without such reasonable belief that you have reached the correct taxpayer or representative, you must not leave any tax or other sensitive information on the message.
- (2) When you can't positively identify the number reached as the taxpayer's or representative's, and it is otherwise proper and practical, simply ask for a return call without giving the taxpayer's name. 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 generally must not identify themselves as IRS unless they reasonably believe the answering machine or voicemail belongs to the taxpayer or representative.

10.5.1.6.8
(09-15-2023)
**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.
- (5) For external electronic communications, IRS personnel should use IRS-approved alternatives to email such as secure messaging or secure portals when available. See IRM 10.5.1.6.8.6, Other Secure Electronic Communication Methods. For more information about emailing outside the IRS, see the following subsections in this IRM for policy about taxpayers and representatives, other external stakeholders, IRS accounts, and personal email.

Note: Different policies apply for emails to taxpayers and representatives, other stakeholders, those with IRS accounts, and personal email. For more information and requirements about emailing outside the IRS, see 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; and 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 name control) in the email subject line.

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

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

- (7) IRS IT-approved encryption technology includes:

- a. **Internal (within the IRS network):**
 - Secure email certificate encryption using the Encrypt with S/MIME option.
 - Secure email encryption using the Encrypt-Only option.
- b. **External (outside the IRS network):**
 - Password-protected encrypted attachments.
 - Previously authorized secure email certificate encryption or secure messaging portal, for example, refer to the *internal LBI Secure Email program site*. For alternatives to email, see 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. Refer to IRM 10.8.52, Information Technology (IT) Security, IRS Public Key Infrastructure (PKI) X.509 Certificate Policy, for more information about secure email certificate encryption.
- c. **Attachments:**
 - SecureZip password-protected encrypted attachments.
 - Document encryption with password protection.

Note: These methods only encrypt the attachment, not the body of the email or the address or subject information. Exclude SBU data from the attached file name(s).

Reminder: Never send the password in the email with the password-protected encrypted attachment.

(8) Refer to these IRMs for more policy:

- IRM 1.10.3, Standards for Using Email.
- IRM 1.15.6, Managing Electronic Records.
- IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, in the Electronic Mail Security and Use of External Information Systems sections.
- IRM 10.8.27, Personal Use of Government Furnished Information Technology Equipment and Resources.
- IRM 11.3.1, Disclosure of Official Information, Introduction to Disclosure, in the Electronic Mail and Secure Messaging section.

10.5.1.6.8.1
(09-15-2023)

Emails to Taxpayers and Representatives

- (1) Unless authorized by this policy in the limited allowable situations listed in this section, 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 LBI and Chief Counsel employees. Refer to the *internal LBI Secure Email program site* and the *Chief Counsel Directives Manual* for more information. For alternatives to email, see IRM 10.5.1.6.8.6, the Other Secure Electronic Communication Methods section.

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 LBI Secure Email program site* or for alternatives to email, see IRM 10.5.1.6.8.6, the Other Secure Electronic Communication Methods section.
 - b. Brief, unencrypted message confirming the date, time, or location of an upcoming appointment, but not the nature of the appointment. Include no SBU data (including PII and tax information, such as name control) in the email, subject line, or attachment. Do not allow follow-up email discussion of any taxpayer account or case.
 - c. 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.
- (4) When responding to unsolicited emails from taxpayers or tax professionals, respond by letter or phone if possible; if address or phone number 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. Sample response:

To ensure your privacy, we discourage you from sending your personal information to us by unencrypted email. Further, 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
(09-15-2023)
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 (see IRM 10.5.1.6.8) only when:
- a. Individual authorized to receive it under law or regulation, such as IRC 6103. Establish authority by a formal request for information processed using established written procedures, or a memorandum of understanding or executed agreement which also establishes email as the secure method of transmission for the data. See IRM 10.5.1.2.10, Authorization.
- Note:** The IRS Office of Safeguards does not authorize agencies subject to Pub 1075 to email tax information (FTI).
- 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*.

- g. For tax information (FTI), sender adheres to policy in the IRM 11.3 series, Disclosure of Official Information.
- h. For non-tax PII, sender adheres to requirements in this IRM and IRM 10.5.6, the Conditions of Disclosure Under the Privacy Act section.

- (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, see 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).
- (5) For those who must provide IRS with their SBU data (such as PII) to facilitate 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
(09-15-2023)

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 that contain SBU data (including PII and tax information) with IT-approved encryption, which includes secure messaging or password-protected encrypted attachments.

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, IT Security Roles and Responsibilities, the Contractor section.

10.5.1.6.8.4
(09-15-2023)

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: In these 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.

- a. Personal Information – You may send your own SBU data (including your PII and your tax information) to or from your personal email accounts, if it is in a password-protected encrypted attachment. Examples may include, but are not limited to:
 - 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 (but only by adding personal email address for ConcurGov notifications related to their own travel, not approvals for others; personnel cannot forward a travel itinerary from a work email address to a personal email address).

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

- b. 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).
- c. 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. Refer to IRM 10.8.60 and IRM 10.8.62. Limit SBU data to that necessary for the situation. Encrypt necessary SBU data in password-protected attachments, if possible, in emergencies. Examples may include, but are not limited to:
 - Sending infectious disease-related documentation to an IRS email account when you do not have other options.
 - Reporting for work.
 - The condition or availability of the workplace.
 - An emergency (internal to IRS, not taxpayer communication).
 - Checking the well-being of IRS personnel.

Note: Other options include, but are not limited to, 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) For more information on continuity management, contingency planning, or disaster recovery, refer to IRM 10.8.60 and IRM 10.8.62.

10.5.1.6.8.5
(09-15-2023)
**Limited Exceptions to
Email SBU Data
Encryption**

- (1) The general rule for encrypting SBU data (including PII and tax information) in emails reflects 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) Having evaluated business needs in relation to potential risk, the following limited exceptions for external emails are appropriate.

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

- (3) Limited exception: Subject line of case-related emails to the Department of Justice.

- a. When IRS personnel communicate with the Department of Justice about established cases, personnel may include the case name and 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. However, 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.
- (4) Limited exception: Emails generated to taxpayers or representatives by approved online applications.
 - a. The IRS online applications may issue emails to taxpayers or representatives, without encryption, when the messages contain only incidental information (**not** tax information, which includes but is not limited to payment amount, address change, or type of notice):
 - 1. To confirm authentication.
 - 2. To inform a user that a secure message is available for viewing on the IRS Secure Messaging Portal.
 - 3. To confirm an online transaction (without details).
 - b. This exception is limited to the following circumstances:
 - 1. The email is automatically generated by an approved IRS application developed by or in conjunction with the Office of Online Services, and
 - 2. 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. For approval of online application email content, email **Privacy*.
- (5) Limited exception: IRS employees sending their personal SBU data via encrypted email or encrypted attachment. Personal SBU data is information pertaining only to you.
 - a. You may choose to send your personal SBU data outside the IRS via encrypted email or a password-protected encrypted attachment.
 - b. You must send this information only if you encrypt the email or attachment(s) and send only your personal SBU data.
 - c. This exception does not include IRS usernames and passwords.
 - d. For policy on encryption, see IRM 10.5.1.6.2, Encryption.
 - e. For more information about when and how to encrypt, refer to the *internal Encryption site*.
 - f. Refer to instructions for using SecureZip to encrypt attachments on the *internal IRS Service Central site*.
- (6) Limited exception: Emergency emails by Facilities Management and Security Services (FMSS).
 - a. Where significant incidents (as defined in IRM 10.2.8, Incident Reporting) 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
(09-15-2023)

**Other Secure Electronic
Communication Methods**

- (1) IRS offers some alternatives to email to protect taxpayer security and privacy:
 - a. Taxpayer Digital Communication (TDC) secure messaging platform: Taxpayers must register, but can then send and receive messages on an encrypted platform. For the internal login page, refer to *Taxpayer Digital Communication (TDC) eGain platform 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, though a notice, phone conversation or in-person visit. This is a one-way (public to IRS) encrypted communication. Refer to the external *IRS Document Upload Tool* 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 section addresses forms of transmission other than phone and email.
- (2) You must provide adequate safeguards for SBU data (including PII and tax information) transmitted from one location to another.

10.5.1.6.9.1
(09-15-2023)

Field and Travel

- (1) If 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 to the extent possible.

Note: Protecting SBU data includes avoiding encounters with smart devices that can record. See 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. If the vehicle does *not* have a trunk, conceal the material from plain view and secure it in some manner. 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).

Note: In either case, lock the vehicle and leave the material unattended for only a *brief period*.

- (3) If you must leave the SBU data (including PII and tax information) unattended in hotel or motel room, lock it in a briefcase and conceal it to the extent possible.
- (4) If SBU data (including PII and tax information) is moved from one building to another (even within the same campus) or one location to another even if it is 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.

Note: 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 taxpayer location when using GPS and location services, see IRM 10.5.1.6.11, Global Positioning Systems (GPS) and Location Services.

10.5.1.6.9.2
(09-15-2023)

Mail through USPS

- (1) IRS personnel must follow proper data protection procedures when mailing SBU data. For more information on IRS policy about mail operations, refer to IRM 1.22.5, Mail and Transportation Management, Mail Operations.
- (2) For telework mail procedures, refer to IRM 6.800.2, the Mail section, and IRM 1.22.5, the Guidance on Telework Employee Mail and the Home as Post-Of-Duty (HaP) Employees section.
- (3) Mail letters and packages with SBU data that weigh less than 13 ounces via United States Postal Service (USPS). These packages do not require double packaging and double labeling. For more information about larger items, see IRM 10.5.1.6.9.3, Shipping through Private Delivery Carrier.
- (4) When sending SBU data by mail **within the U.S. and Territories** (served by United States Postal Service [USPS]):
 - a. Place SBU data in a single opaque envelope/container.
 - b. Seal it to prevent inadvertent opening and to reveal evidence of possible tampering.
 - c. Clearly show the complete name and address of the sender and intended recipient or program office on the envelope/container.

Note: Mailroom personnel may open and examine SBU data the same way they evaluate and determine 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 (i.e., APO/FPO), 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, DPO, etc.
 - 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 ensure delivery at the final destination meets Treasury/IRS needs and DOS schedule for such deliveries.

10.5.1.6.9.3
(09-15-2023)

**Shipping through
Private Delivery Carrier**

- (1) IRS personnel must follow proper data protection procedures when shipping PII 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 impacted individuals.
- (2) For Telework shipping procedures, refer to IRM 6.800.2, the Mail section, and IRM 1.22.5, the Guidance on Telework Employee Mail and the Home as Post-Of-Duty (HaP) Employees sections.
- (3) Mail letters and packages with PII that weigh less than 13 ounces via United States Postal Service (USPS). These packages do not require double packaging and double labeling. See IRM 10.5.1.6.9.2, Mail through USPS.
- (4) You must ship packages with PII that weigh 13 ounces or more through a private delivery carrier.
- (5) 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, the Media Transport section.

Note: The IRS restricts the ability to save data on removable media storage devices. Refer to IRM 10.8.1, the Media Use section, and *removable media guidance* on the *internal IRS Service Central site*.

- (6) For all PII 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 impacted 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 retains 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, DPO, etc.

- (7) When shipping PII 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.

- (8) CampusShip allows employees to:
 - a. Generate labels electronically.

- b. Secure current IRS address information from 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 PII loss or disclosure to an unauthorized individual.
 - d. Let recipients know a package is coming by adding their email address to CampusShip for notifications.
- (9) You must double-package and double-label PII packages prior to 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.

- (10) Evaluate the size of the PII shipment and identify appropriate packing materials. The proper type of internal and external packaging depends upon the size and weight of the package. Use the smallest size packaging possible to reduce shipping costs and ensure minimal shifting of contents during shipment.
- (11) The sender must also decide whether to ship via ground service or express (Overnight and Second Day Air) services:
- Use **Ground service** for shipping whenever possible. Ground service should always be the first choice; use express services only when necessary. There is no requirement to mail PII 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.
- (12) For all PII 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 PII and asking for recipient acknowledgement. This practice includes shipments to IRS offices, contractors, external agency partners, and even taxpayers (or their representatives, referred to collectively as taxpayers) when applicable. For external partners and taxpayers, 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 impacted 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 impacted 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 an official letter is used as Form 3210 equivalent, the SSN may not be present. Ensure that enough information is available on the letter to identify impacted individuals in case of loss or disclosure.

- (13) Securely package the PII by placing the contents and the properly completed Form 3210 (or equivalent) in an appropriately 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 prior to shipment that the package with PII is on its way. 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.

Note: When you send duplicate packages to a taxpayer and their representative, either may acknowledge receipt for both packages.

- (14) Internal packaging may include any of the following:
- **An envelope:** An E-20, Confidential Information envelope, is acceptable for this purpose.
 - **A plastic bag:** Should be sturdy enough to support the weight of the contents without tearing; should be black, green, or a similar color so the contents are not readable through the plastic bag.

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.

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

- (15) Label the internal package with the following information:
 - a. Send to Address, including Mail Stop and/or Drop Point Number, if applicable.
 - b. Return Address, including Mail Stop and/or Drop Point Number, if applicable.
 - c. Sender's phone number.
 - d. Small Carrier tracking number, if available.
 - (16) The sender may use a copy of the exterior small package carrier shipping label for the internal label, so print 2 copies (the first for the interior, the other for the exterior).
 - (17) 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 maximum 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, combined 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 get caught on conveyer belts and damage or destroy the shipment.
- (18) Whenever possible, use a new box; however, you may re-use undamaged packaging materials to ship PII. 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.
 - (19) 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/or commercially bought Styrofoam peanuts, air bags, etc.
 - c. Place the cushioning material around the items in the box. Close and shake the box to see whether you have enough cushioning material; add more cushioning material if you hear or feel the contents shifting.
- (20) 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, but are not limited to:
- “Remittance” labels indicating 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 IRS from an envelope since it is necessary to include IRS on Return Address and Send To Address labels to ensure package delivery to the intended location if any of the address information is incorrect.

- (21) 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, and/or plastic straps.
- (22) Place the shipping label on the top of the package and ensure it is properly adhered 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.
- (23) The sender must monitor the shipment delivery. Follow your organization’s established time frames for Form 3210 (or equivalent) acknowledgement follow-up. Where there is no established 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.
- (24) 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 prior to 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.

- (25) After receiving the acknowledgement copy (if applicable, equivalent confirmation of receipt), the sender will associate it with the original Form 3210 (or equivalent).

Note: 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).

- (26) If you do not receive the signed Form 3210 acknowledgement (or equivalent confirmation of receipt) within the established time frame, access the small package carrier's website to track the shipment to find if it was delivered successfully. The tracking number should have been included on Form 3210 (or equivalent) when the shipping labels were prepared or after the number was received from the carrier if Form 9814 was used.
- (27) If the tracking information shows the package **was delivered**, 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.

Note: 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.
- (28) If the tracking information indicates the package **was not successfully delivered**, the sender should closely monitor the tracking information for up to 48 hours (2 business days) after the anticipated delivery date for air services and up to 72 hours (3 business days) after the anticipated 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.
- (29) Immediately upon discovering or identifying a package is lost, report the loss following IRM 10.5.4. Refer to the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.
- (30) Business unit management must establish an internal process to identify the package contents and impacted 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 determine if it belongs to the IRS. You must provide detailed information about the contents such as taxpayer last names, check numbers, forms numbers, documents enclosed, etc., including any and all identifying information that might help locate the contents of the package.
- (31) Managers must perform, at a minimum, quarterly audits of the Form 3210 (or equivalent) acknowledgement process for packages with PII to ensure proper follow-up is occurring. Managers must document the results of these audits. This procedure will allow IRS managers the opportunity to confirm that PII 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 PII 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.

- (32) Additionally, management should periodically sample mail to ensure the business unit follows this PII shipping policy.
- (33) For more information, refer to the *PII Hardcopy Shipping*.
- (34) Refer to IRM 1.15.5, Relocating/Removing Records, for shipping records (such tax or personnel records) to the Federal Records Centers.

10.5.1.6.9.4 (09-15-2023)

Faxing

- (1) Protect faxed SBU data (including PII and tax information) as with any other transmission of SBU data.

Note: For detailed procedures on how to safely fax sensitive information, including to taxpayers and their authorized representatives, refer to IRM 21.1.3, the Mailing and Faxing Tax Account Information section. Also refer to the *internal Faxing site*.

- (2) 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. See IRM 10.5.1.6.8, Email.
- (3) If you must fax the information, do not send SBU data to a fax machine without contacting the recipient to arrange for its receipt.
- (4) Use a cover sheet for faxes with SBU data that lets the recipient know that it contains sensitive information and requests unintended recipients to report the disclosure and confirm destruction.
- (5) For misdirected faxes, refer to IRM 10.5.4, Incident Management Program, the Responsibilities section.
- (6) When transmitting SBU data via fax, use Enterprise Electronic Fax (EEF) as the preferred method of faxing documents. Refer to IRM 21.2.3, Systems and Research Programs - Transcripts (the IRS Electronic Fax System section) or the *internal EEFax site*.
- (7) For more information on securely faxing documents, refer to IRM 10.8.1, the Facsimile and Facsimile Devices and AC-20 Use of External Information Systems - Control Enhancements sections.

10.5.1.6.9.5 (09-15-2023)

Printing

- (1) Protect printed documents with SBU data and follow the IRS Clean Desk Policy in all work locations (including field and telework).
- (2) Minimize the printing of SBU data to what is explicitly necessary.
- (3) Properly store and dispose of printed materials. See 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, the Printers, AC-20 Use of External Information Systems, and Personally-Owned and Other Non-Government Furnished Equipment sections.

10.5.1.6.9.6 (09-15-2023)

Text Messaging (Texting)

- (1) IRS personnel must not use text messaging (texting) for official business.

- (2) Refer to IRM 1.15.6, Managing Electronic Records, the Use of Agency-approved Electronic Messaging Systems, Preserving Electronic Messages, and Common Questions about Electronic Messaging sections.
- (3) Refer to IRM 10.8.1, the Telecommunication Devices section.

10.5.1.6.9.7
(09-15-2023)
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 blacklisted sites.

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

- (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: However, this policy does not apply to SBU data the IRS proactively makes available to all IRS personnel on internal resource sites (including, but not limited to, Discovery Directory, Outlook (calendar, profile information, and address book), intranet, 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) For receiving documents from taxpayers, IRS personnel may offer taxpayers the opportunity to use the *Document Upload Tool (DUT)* when this option is available. For more information about when you can offer this tool, refer to your business unit procedures.
- (5) For internal collaborative electronic or online data sharing, see 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).
- (6) For more information about securing electronic transmissions, refer to IRM 10.8.1, the AC-20 Use of External Systems, the SA-9 External System Services, and the External Collaborative Technology and Systems sections.
- (7) For more information about secure emailing, see IRM 10.5.1.6.8, Email.

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. Maintain accountability to ensure 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
(09-15-2023)
**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 types 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, but is not limited to, 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; however, 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). The fact that material has been 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. See 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 ensure employees discard sensitive waste material properly.

10.5.1.6.10.1
(09-15-2023)
**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/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/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]

Note: When shredding, you must procure and use the same equipment approved for destroying Secret and/or Confidential classified information (CNSI). See the current *National Security Administration/Central Security Service (NSA/CSS) Evaluated Products List (EPL)* for compliant shredders. [TD P 15-71, Treasury Security Manual, Chapter III, Section 16, Destruction of Classified and Sensitive Information]

- (3) For multi-step destruction of paper, you may use non-compliant methods for the first step. The IRS must then protect the product until it is then destroyed in a manner that renders it unreadable, indecipherable, and irrecoverable. [32 CFR 2002]

10.5.1.6.10.2
(09-15-2023)
**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, the MP-6 Media Sanitization section, and follow NIST SP 800-88, Guidelines for Media Sanitization.
- (2) Refer to the *internal Media Destruction Shipping Procedures site* on 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
(09-15-2023)
**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. Ensure burn bags or shred boxes only are collected and contents destroyed by cleared contractor personnel or facilities maintenance personnel, or persons authorized by IRS privacy, records, or security officials.
 - 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 located 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
(09-15-2023)
**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.

Note: An approved Form 11671, Certificate of Records Disposal for Paper or Electronic Records, is required prior to destruction of any original federal records. Refer to IRM 1.15.3, Records and Information Management, Disposing of Records.
- (2) Disposition and destruction of tax information must follow the Records and Information Management IRM 1.15.2, Types of Records and Their Life Cycle, IRM 1.15.3, Disposing of Records, and IRM 1.15.6, Managing Electronic Records.

10.5.1.6.10.6
(09-15-2023)
**Contractors Disposition
and Destruction**

- (1) Turn over unshredded sensitive information to a contractor provided the contract includes necessary safeguards that ensures compliance with 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, Disclosures to Contractors, the Destruction of Returns and Return Information section.
- (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 maintain certification designation with an industry trade association that conducts scheduled and unannounced site inspections and reports out on findings. periodically review work areas to ensure that contractors are discarding sensitive waste material properly.
- 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 maintaining 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
(09-15-2023)
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 it is 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 the event the device is lost or stolen.
- (5) Take every precaution to prevent the GPS device from being left unattended or unsecured.
- (6) Remove portable GPS devices from vehicle when not in use as circumstances allow. In those limited instances 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 mount, clean the suction cup mount area because it can leave marks on the windshield/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 breach of PII:
 - a. Immediately upon discovery of the loss or theft, the employee must report the potential breach to the employee's manager and the appropriate organizations based on what was lost or disclosed.
 - b. For more information about how to report an incident, refer to IRM 10.5.4, Privacy and Information Protection, Incident Management Program, or the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.

10.5.1.6.11.2
(09-15-2023)
Location Services

- (1) Except for the use of GPS in IRM 10.5.1.6.11.1, 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 (Facebook Check In, Find My Friends, etc.). 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
(09-15-2023)
Telework

- (1) Special privacy considerations 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 section.

- (2) Except for those documents received in a field environment, do not take high security items (see 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, Employee Benefits, IRS Telework Program.
- (4) For telework mail procedures, refer to IRM 6.800.2, the Mail section, and IRM 1.22.5, the Guidance on Telework Employee Mail section.
- (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, the Equipment and Furniture section.
- (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, the AC-18 Wireless Access section.

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

- (8) Teleworking personnel should adhere to 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 consider:
 - a. If possible, set home office designated 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/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. Whenever 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. See 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 transmit SBU data, follow IRM 10.5.1.6.9, the Other Forms of Transmission section 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, see IRM 10.5.1.6.10, Disposition and Destruction.

Note: Bring all SBU data for destruction into the office for proper disposition.

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

10.5.1.6.13
(09-15-2023)
**Bring Your Own Device
(BYOD)**

- (1) Bring Your Own Device (BYOD) is a concept that allows personnel to utilize 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/or data on their personal tablets/e-readers, smartphones, and other devices.

- (2) To protect the privacy of the tax information, BYOD participants must:
- Use only IRS-approved applications.
 - Refrain from using devices in public settings where others might overhear conversations involving SBU data (including PII and tax information) or where others might see screens with this information. See IRM 10.5.1.6.7.1, Cell Phone and Cordless Device.
 - Follow the terms in the Personally-Owned Mobile Device Acceptable Use Agreement, including, but not limited to:
 - 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.
 - Adhere to 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.

Note: This program protects the privacy of the taxpayer. 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, the System Use Notifications section.

- (3) 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.”

- (4) 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.
- (5) For more information about BYOD, refer to the *internal BYOD site*.

10.5.1.6.14
(09-15-2023)
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 guarantees civil liberties: <https://www.archives.gov/founding-docs/bill-of-rights>
- (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, the Privacy Act Recordkeeping Restrictions (Civil Liberties Protections) section.
- (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. See IRC 7803(a)(3), Execution of Duties in Accord with

Taxpayer Rights. For more information about the TBOR, see <https://www.irs.gov/taxpayer-bill-of-rights>. The TBOR requires the IRS to protect taxpayer rights to privacy (with due process) and confidentiality as essential rights that help protect their civil liberties:

<https://www.irs.gov/taxpayer-bill-of-rights>

- (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 (see IRM 10.5.1.6.14.3, Monitoring Individuals).
- (8) Refer to IRM 10.5.2 for more information on the PCLIA process.
- (9) For more information, refer to IRM 10.5.6, the Privacy Act Recordkeeping Restrictions (Civil Liberties Protections) section.
- (10) For more information, refer to *TD P 25-04 Privacy Act Handbook*, the Record Keeping Under the Privacy Act section.

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.
- (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 a particular 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 maintaining 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, in some instances, 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. [Privacy Act; Purpose Limitation]
- (7) For more information, refer to IRM 10.5.6, the Privacy Act Recordkeeping Restrictions (Civil Liberties Protections) section.

10.5.1.6.14.2
(09-15-2023)

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, but not limited to, video, photographic, or infrared) in the workplace center around individual employee privacy, the potential disclosure of SBU data (including PII and tax information), and data minimization and retention. [Minimizing Collection, Use, Retention, and Disclosure]
- (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.

Note: IRC 7521 applies to recording taxpayer interviews, as described below in the Business need section.

- (4) To record in the workplace, you need:
 - a. Business need [Minimizing Collection, Use, Retention, and Disclosure]
 - b. Approval [Accountability]
 - c. Consent [Openness and Consent]
 - d. Precautions [Strict Confidentiality]
- (5) **Business need:** Minimize recordings in the workplace unless you have a compelling business need. Just referring to notes to refresh your memory after a meeting is not a reason to record.
- (6) Examples of compelling business need that allows for limited recording in the IRS workplace with approval and consent include, but are not limited to:
 - a. **Service Quality Control:** Employees may make recordings when performed to determine the quality of service delivery, such as with Contact Recording.
 - b. **Taxpayer Interviews:** 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, the IRS Initiated Audio Recordings section.
Refer to the Requests to Audio Record Interviews section of IRM 4.10.3, Examination of Returns, Examination Techniques; to the Taxpayer Recording of Interviews section of IRM 5.1.12, Field Collecting Procedures, Cases Requiring Special Handling; and to the Right to Make an Audio Recording of the Proceeding section of IRM 25.5.5, Summons, Summons for Taxpayer Records and Testimony.

Caution: Taxpayers do not have the right to record phone (including online meeting) interviews. If you know a taxpayer call is being recorded by a party other than the IRS (such as a prison recording an incarcerated taxpayer), end the call as described in the Taxpayer Request to Tape Record Conversation section of IRM 21.1.3.

 - c. **Investigation:** 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).

- d. **Employee Education:** When used for employee education, employees may make recordings using IRS-issued software applications or platforms, such as Adobe Articulate, Teams, or Saba Centra.
- e. **Reasonable Accommodation:** 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, Equal Employment Opportunity and Diversity, Providing Reasonable Accommodation for Individuals with Disabilities.
- f. **Labor Relations:** 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, Labor-Management Relations; IRM 6.751, Discipline and Disciplinary Actions; IRM 6.752, Disciplinary Suspensions and Adverse Actions; and IRM 6.771, Agency Grievance System.

Note: These recordings will be federal records. For more information about where these federal records must reside, refer to the IRM 1.15 series, Records and Information Management, Files Management.

(7) **Approval:**

- a. For IRS-initiated audio recordings with taxpayers, Field Territory manager approval is required. Refer to IRM 4.10.3, the IRS Initiated Audio Recordings section.
- b. For physical security reasons, IRS personnel must not conduct photography without prior FMSS approval in IRS facilities or at alternative duty stations duties remote to the conventional office site (e.g., satellite locations, employee's residence). Refer to IRM 10.2.14, the Photography and Video Recordings Prohibition section.

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. 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, IRS Privacy Act Consent. Refer to IRM 10.5.6, the Privacy Act Consent for Disclosure section.

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

(9) **Precautions:**

- a. Take precautions that no unauthorized recordings or disclosures occur. 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 phones, tablets, etc.). For more information about precautions, see IRM 10.5.1.6.20, Smart Devices, about digital assistants, smart devices, IoT, and other devices that can record or transmit sensitive audio or visual information.

- b. 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). Ensure those items are not in view or earshot of the device.
- c. 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).

10.5.1.6.14.3
(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]
- (2) However, limitations still exist on use of any PII collected, with sharing on a need-to-know basis for its intended use only. [Privacy Act]
- (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, the Privacy Act Recordkeeping Restrictions (Civil Liberties Protections) section.
- (5) The IRS PCLIA addresses these limitations. For more information about PCLIA's, refer to IRM 10.5.2, Privacy Compliance and Assurance (PCA) Program.

10.5.1.6.15
(09-15-2023)
Contractors

- (1) The IRS defines as personnel as including contractors in IRM 10.5.1.1.2, Audience, so they must also follow the requirements in IRM 10.5.1.4.1, Employees/Personnel.
- (2) The IRS has privacy obligations for contractors with access to SBU data (including PII and tax information). As outlined in the IRS Privacy Principle of Accountability and NIST Privacy Controls, the IRS must:
 - a. Establish privacy roles, responsibilities, oversight, and access requirements for contractors and service providers throughout the privacy lifecycle. [OMB A-130]
 - b. Include privacy requirements for all relevant stages of the privacy lifecycle in contracts and other acquisition-related documents, including end of contract.
 - c. Follow Privacy Act requirements for contractors, outlined in IRM 10.5.6, the Privacy Act Contract Requirements section.
- (3) Employees responsible for procurement activities on contracts that involve SBU data (including PII and tax information) must meet the requirements in IRM 10.5.1.4.7, Personnel Engaged in Procurement Activities.

10.5.1.6.16
(09-15-2023)

**Online Data Collection
and Privacy Notices**

- (1) Online data collection may require several types of notices:
 - a. An IRS-approved IT system use notification message (refer to IRM 10.8.1, the AC-8 System-Use Notifications section).
 - b. Link to IRS.gov Privacy Policy (see that section in IRM 10.5.1.6.16.1).
 - c. An online data collection website or application Privacy Policy notice (see that section in IRM 10.5.1.6.16.2).
 - d. Privacy Departure Notice (see that section in IRM 10.5.1.6.16.3).
 - e. Privacy Act Notice (if collecting data on an online form). Refer to IRM 10.5.6, the Privacy Notices section.
- (2) Do not use persistent cookies or other tracking devices to monitor the public's visits on an IRS internet site, except as authorized by OMB regulations.
- (3) For questions or Privacy Policy notice review or approval, email **Privacy*.
- (4) For more information on authentication of individuals in online transactions, see IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA).

10.5.1.6.16.1
(09-15-2023)

**IRS.gov Privacy Policy
Notice**

- (1) The IRS internet privacy policy notices on IRS.gov inform the public of the information collection procedures and the privacy measures in place for a particular internet website or activity. [OMB-10-23, E-Government Act, OMB A-130, OMB-03-22, Openness and Consent, PT-5]
- (2) Link to the *IRS Privacy Policy* at every major entry point to an IRS internet website or application, as well as on any page collecting substantial personal information from the public. The requirement also may include a unique privacy policy for that website. See IRM 10.5.1.6.16.2, Online Data Collection Website or Application Privacy Policy Notice.
- (3) The IRS privacy policy notice is:
 - a. An overview of IRS privacy practices.
 - b. A description of any information collected and stored automatically by the system and how the IRS will use this information.
 - c. An explanation of how the IRS will use any PII submitted by the internet visitor.
 - d. A notice that security and intrusion protection measures are in place.
- (4) Refer to the overarching IRS.gov Internet Privacy Policy notice:
<https://www.irs.gov/privacy>

10.5.1.6.16.2
(09-15-2023)

**Online Data Collection
Website or Application
Privacy Policy Notice**

- (1) A unique privacy policy for a website or application must detail the differences from the IRS.gov privacy policy. This policy applies to any website or application hosted by or for the IRS. [OMB-10-23, E-Government Act, OMB A-130, OMB-03-22, Openness and Consent, PT-5]

Note: If the website or application is asking for SBU data (including PII or tax information), then the website or application needs to explain its use of the data.

- (2) The website or application privacy policy must still link to the *IRS.gov Privacy Policy*.
- (3) A simple example or template, with brackets *[like this]* to fill in the details pertinent to the website or application, is:

[Name of website or application] Privacy Policy Notice

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

- (4) If the website or application is more complex, you might need a more complicated policy notice.
- (5) For questions or Privacy Policy notice review or approval, email *Privacy.

10.5.1.6.16.3
(09-15-2023)

Privacy Departure Notice

- (1) Any IRS internet website (or link to a third-party site for the IRS) that links to external sites that are not part of an official government domain must post a privacy departure notice. This notice alerts internet visitors that they are about to leave the IRS website and its privacy practices. It advises them to review the website privacy practices for the website they are about to enter. [OMB-10-23, E-Government Act, OMB A-130, OMB-03-22, Openness and Consent, PT-5]

Note: OMB does not require privacy departure notices for sites that are part of an official government domain. However, for transparency and because the IRS often has tax information and we want to maintain public trust, we recommend that all links to external sites use a privacy departure notice.

- (2) The privacy departure notice must be a pop-up or a statement adjacent to the link.
- (3) For the departure notice language, you can use:
You are leaving the IRS website. Protect your privacy. Review the privacy policy available on the websites you are visiting and be cautious about providing your personal information.
[Continue] [Cancel]

Note: As long as you make these points, you can modify this language to reassure visitors that these links take them to approved partners.

10.5.1.6.16.4
(09-15-2023)

Intranet or Non-Publicly Accessible Privacy Policy and Departure Notice

- (1) IRS intranet or non-publicly accessible privacy policy notices inform personnel of the information collection procedures and the privacy measures in place at a particular intranet site or activity. This notice is a modified version of the IRS.gov Privacy Policy Notice; see IRM 10.5.1.6.16.1. [OMB-10-23, E-Government Act, OMB A-130, OMB-03-22, Openness and Consent, PT-5]

- (2) Link to the *internal IRS intranet privacy policy notice* at every major entry point to an intranet site, as well as on any page collecting personal information from an individual.
- (3) Any IRS intranet site or page that links to external sites that are not part of an official government domain must post a privacy departure notice. This notice alerts IRS personnel that they are about to leave the IRS website and its privacy practices. It advises them to review the privacy practices on the website that they are about to enter. This is a modified version of the privacy departure notice; see IRM 10.5.1.6.16.3.
- (4) For the intranet departure notice language, you can use:
You are leaving the IRS intranet. Protect your privacy. Review the privacy policy available on the websites you are visiting and be cautious about providing your personal information.
[Continue] [Cancel]
- (5) Do not use persistent cookies or other tracking devices to monitor an individual's visit to IRS intranet sites, except as authorized by OMB regulations.

10.5.1.6.17
(09-15-2023)
Social Media

- (1) The IRS uses social media to share the latest information on tax changes, initiatives, products, and services. To expand reach to taxpayers and stakeholders, the IRS shares information on several social media platforms, including Twitter, Facebook, and LinkedIn.
- (2) Because the use of social media allows potential direct interaction with the public, the IRS implemented specific rules to ensure only authorized employees speak in an official capacity. 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 *internal Rules of Behavior*.
- (3) For more information about internet research guidelines, refer to IRM 11.3.21, Requirements for Investigative Disclosure, the Use of Social Networking and Other Internet Sites by IRS Employees for Compliance Research or for Other Purposes section.
- (4) Personal, non-work usage of these social media tools on personal devices must not compromise the confidentiality of SBU data (including PII or tax information) or the integrity of the IRS. Except for approved IRS communicators handling official IRS media initiatives, the IRS does not authorize you to use social media in an official capacity and should follow the Communications and Liaison guidelines. 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 appropriate social media authorization form or contact the appropriate social media platform owner.
- (6) If an IRS organization would like to consider use of a new social media platform, they must submit 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 PCLIAs, refer to IRM 10.5.2, Privacy Compliance and Assurance (PCA) Program.

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, but not limited to, Discovery Directory, Outlook (calendar, profile information, and address book), intranet, and Share-Point or Teams site collections), such as names and business contact information.
- (2) Some of the privacy risks associated with collaborative data sites include:
 - a. 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 residing 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, the SC-15 Collaborative Computing Devices section.
- (4) Refer to IRM 10.8.1, the SC-15 Collaborative Computing Devices section.

10.5.1.6.18.1
(09-15-2023)
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, reminders, etc. 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 that contain SBU data (including PII and tax information) other than noted in the following sections.

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, but not limited to, Discovery Directory, Outlook (calendar, profile information, and address book), Intranet, and SharePoint or Teams site collections), such as names and business contact information.
- (4) For **Business Unit Calendar Meetings/Appointments about Taxpayers**:
 - a. Place on the calendar only a portion 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).
 - b. The abbreviated name should consist of the first four significant characters of the taxpayer entity's name (the name control):
 - i. 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.

ii. 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").

(5) For **Calendars for Offices with Regulatory, Investigative, and/or Advocacy Responsibilities** (docketed case meetings):

- a. These requirements apply to calendars for Appeals, Chief Counsel (Counsel), Criminal Investigation (CI), Taxpayer Advocate Service (TAS), and other functions with regulatory, investigative, and/or advocacy responsibilities.
- b. 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, the Information Which Has Become Public Record section.)

- c. 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.

(6) For **Calendars for Offices with Regulatory, Investigative, and/or Advocacy Responsibilities** (taxpayer meetings):

- a. 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 (see earlier section), 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.
- b. CI may use the Criminal Investigation Management Information System (CIMIS) investigation number.
- c. 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.

(7) For **Non-Taxpayer-Related Meetings/Appointments**:

- 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 appropriate), and/or 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 encrypted, password-protected attachments using IT-approved encryption methods) with directions in the calendar invite to look for the separate email.
- c. Examples of situations where you may use this practice include, but are not limited to:
 - i. Where Counsel hosts informational meetings with external parties, such as trade groups or other professional organizations, in conjunction with its published guidance program.
 - ii. Where IRS organizations meet with external parties to plan or deliver presentations or for procurement matters.
 - iii. Examples of emails requiring encrypted PII or SBU data attachments in these scenarios include details on speakers (such as resumes) or procurement issues (such as contract information).
- d. You may voluntarily include your personal appointments on the calendar to ensure 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. However, 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
(09-15-2023)
Online Meetings

- (1) Online meeting tools include M365 Teams, Saba Centra, Zoom for Government (ZoomGov), etc. Use only enterprise-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 (Zoom.us) application is not an Enterprise Architecture-approved tool.

Caution: 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.

- (2) When using approved virtual meeting tools with encrypted communication capability 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 people from the meeting. See IRM 10.5.1.2.9, Authentication.
 - b. **Authorization:** Make sure the people on the meeting are authorized to hear or view the information. See 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. See 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 con-

versation. You may also conduct a conversation away from passers-by. Be careful not to convey sensitive information that others might overhear.

- d. 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.
- e. Avoid recording meetings. Before recording online meetings, you must have a legitimate business need, proper approval, and prior consent from all parties. See IRM 10.5.1.6.14.2, Recordings in the Workplace.
- f. Meeting hosts (organizers, co-organizers) hold responsibility for controlling the meeting environment, such as removing unauthorized parties, muting audio or video when appropriate to protect privacy, giving notice and getting consent for recording, promoting others as presenters or co-organizers to help moderate the meeting and chat, 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.

- g. Use IRS contact information (such as email or name).
- h. 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. See IRM 10.5.1.6.8.4, Emails with Personal Accounts.

- (3) IRS-approved encrypted online meeting tools may convey SBU data; however, apply the principles of authentication, authorization, and need to know.
- (4) To protect your own privacy, keep chats, profile pictures, and background images professional.
- (5) To prevent inadvertent disclosure, verify which chat or meeting window you are using to ensure you do not put SBU data in the wrong conversation.
- (6) For more information about online meeting privacy considerations, refer to the *internal Online Meeting Tools - Privacy Considerations site*.
- (7) For best practices and answers to questions about using M365 tools, refer to the *internal M365 site*.
- (8) Refer to IRM 10.8.1, the SC-15 Collaborative Computing Devices section.

10.5.1.6.18.3
(09-15-2023)
**Shared IRS Storage
(OneDrive, SharePoint,
Teams, and Other IRS
Collaborative Sites)**

- (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 site) might offer valuable benefits while having 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, see IRM 10.5.1.6.9.7, Electronic and Online.

- (2) Collaborative environment owners also must ensure their users follow rules and protect privacy.

Caution: 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.

- (3) 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* to ask if you need a system PCLIA.
- (4) For more information, refer to IRM 10.5.2, Privacy Compliance and Assurance (PCA) Program, the Privacy Compliance in Collaborative Environments and the System PCLIA sections.
- (5) For more information, refer to IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance (the SC-15 Collaborative Computing Devices and Applications and the SC-28 Protection of Information at Rest sections), and IRM 2.25.20, Integrated Enterprise Portal-Web Services - SharePoint.

10.5.1.6.18.4 (09-15-2023) 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 the ELC and OneSDLC). For more information about OneSDLC, refer to IRM 2.31.1, Lifecycle Management - One Solution Delivery Life Cycle Guidance, or the *OneSDLC site*.
- (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, but are not limited to:
 - 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, etc.)?
 - 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 clauses, including those for protecting SBU data (including PII and tax information)?
 - How long must the data be kept? When will it be destroyed?

- (4) Except for systems principally supporting overseas Federal/Treasury personnel and/or activities, Treasury systems must be located and operated within the U.S. [TD P 85-01, control SA-4_T.193]

Note: This includes Treasury contractor systems.

- (5) PGLD and COR must provide written notification to the contractor when the contractor is allowed to keep Government data at a location outside the U.S.
- (6) Failure to follow privacy and security policies and processes might require contract modifications.
- (7) For more information on cloud computing issues and cloud deployment models, refer to IRM 10.8.24, Information Technology (IT) Security, Cloud Computing Security Policy, and IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance.

10.5.1.6.19
(09-15-2023)
Training

- (1) Although IRC 6103(h) (1) permits 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.
 - 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 compliance with 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, Learning and Education, Learning and Education Policy, the Disclosure Requirements section.
- (3) For more information about training material and marking requirements, see IRM 10.5.1.6.5, Marking, and refer to the Disclosure Requirements, Ethics and Privacy, and Personally Identifiable Information (PII) sections of IRM 6.410.1.
- (4) For official use only requirements, refer to IRM 11.3.12, Designation of Documents, the Protection of Return Information section.

10.5.1.6.20
(09-15-2023)
Smart Devices

- (1) Do not allow digital assistants, smart devices, Internet of Things (IoT), and other devices that can record or transmit 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/or 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 and/or transmit data when activated.
 - b. When working with sensitive data, to protect privacy, personnel must mute or disable the listening/detecting features of the device so they 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) These devices/applications include (but are not limited to the examples provided):
 - Digital assistants (such as Dot or Echo hardware using Alexa software, HomePod using Siri, etc.).
 - Voice-activated devices and smartphone applications (such as Siri, Google Now ("Okay Google"), or Alexa on phones, tablets, etc.).
 - Wearable devices (fitness trackers, smart watches, etc.).
 - Non-IRS-approved video-chatting apps (FaceTime, SnapChat, etc.).
 - Internet of Things (IoT) equipment (devices, systems, etc.), which might include appliances, thermostats, vacuums, lights, etc.
 - Internet-connected toys (robots and AI toys, educational toys, etc.) that might record (video and/or audio) and transmit.
 - Smart TVs or auxiliary audio/visual equipment (if includes voice activation).
 - Operating systems/applications (such as Windows 10, Cortana, etc.) that allow voice commands.
 - Home surveillance, security, and video/audio: Webcams on personal devices in the home, security cameras/microphones.
- (3) For more information about location-related concerns, see IRM 10.5.1.6.11.2, Location Services.

10.5.1.6.21
(09-15-2023)
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. However, biometric technology can be used effectively with proper controls.

- (2) Biometric technology is a combination of the use of very sensitive personal information with automated analysis, frequently 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*, including:
 - a. *NISTIR 7316*, 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*, 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. See IRM 10.5.1.3.2.1.
 - b. **Purpose Limitation:** Biometrics may only be collected for a legitimate IRS purpose. See 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 it is no longer needed. See IRM 10.5.1.3.2.3.
 - d. **Openness and Consent:** Clearly notify individuals whose data is analyzed that their biometric data is being used, how it will be used and safeguarded, and their options should they choose not to use the application. See IRM 10.5.1.3.2.4.
 - e. **Strict Confidentiality:** Only allow access to biometric data by individuals with a need to know it. See 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. See 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. See IRM 10.5.1.3.2.7.
 - h. **Verification and Notification:** Whenever possible, confirm the accuracy of biometric data from the originating source or a reliable, verifiable alternative. See IRM 10.5.1.3.2.8.
 - i. **Access, Correction, and Redress:** Provide individuals enough information to understand their right to review biometric information IRS collects

and options for participating in the process of maintaining its accuracy.
See IRM 10.5.1.3.2.9.

- j. **Privacy Awareness and Training:** Provide IRS personnel and vendors who utilize biometric data with the necessary awareness and training that will guide them to effective privacy decisions. See 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, see IRM 10.5.1.4.4, System Owners, and IRM 10.5.1.4.6, Authorizing Officials (AOs).

10.5.1.7
(09-15-2023)
**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. Because of the complexity, scope, and importance of privacy to the IRS mission, PGLD is not the single point of contact for all privacy-related programs.
- (3) PGLD participates in various privacy-related governance boards.
- (4) This IRM and IRM 10.5.2, Privacy Compliance Assurance (PCA) Program, provide 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 appropriate. This includes, but is not limited to, the following privacy-related programs, not all which PGLD manages.
- (5) For more information about PGLD, refer to IRM 1.1.27, Organization and Staffing, 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) Privacy Policy and Knowledge Management (PPKM), within PGLD's PPC, 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 Chief Privacy Officer's (CPO) 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 appropriate. See 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
(09-15-2023)
**Privacy and Civil
Liberties Impact
Assessment (PCLIA)**

- (1) Privacy Compliance and Assurance (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. [OMB A-130]
- (2) If the IRS procures, uses, or develops IT to process PII, the IRS must consider the privacy protections with a PCLIA. [E-Government Act]

Note: The IRS requires PCLIA 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 and IRM 2.16.1.

- (3) For more information about the PCLIA process, refer to IRM 10.5.2, Privacy Compliance and Assurance (PCA) Program, or the *internal PCLIA site*.

10.5.1.7.3
(09-24-2020)
**Business PII Risk
Assessment (BPRA)**

- (1) Privacy Compliance and Assurance (PCA), within PGLD's PPC, uses the Business PII Risk Assessment (BPRA) program to assess 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 about the BPRA program, email **Privacy* or refer to the *internal BPRA site*.

- 10.5.1.7.4
(09-15-2023)
Privacy Reporting
- (1) Refer to IRM 10.5.6, the Privacy Act Reports section, and IRM 10.5.2, the Reporting section.
 - (2) For more information about privacy reporting, email **Privacy*.
- 10.5.1.7.5
(09-24-2020)
Unauthorized Access (UNAX)
- (1) Information Protection Projects (IPP), under PGLD's Identity and Records Protection (IRP), administers the Unauthorized Access to Taxpayer Accounts (UNAX) program.
 - (2) The term UNAX is used to define the act of committing an unauthorized access, attempted access, or inspection (commonly referred to as UNAX) of any tax information contained on paper or within any electronic format without a management-assigned IRS business need.
 - (3) For more information, refer to IRM 10.5.5, IRS Unauthorized Access, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements.
 - (4) Refer to the *internal UNAX site*.
- 10.5.1.7.6
(12-31-2020)
Mandatory Briefings
- (1) Mandatory briefings deliver required IRS-wide training – including the Privacy Information Protection and Disclosure, Records Management, and UNAX briefings managed by the PGLD offices of PPKM, IRP, and IPP, respectively.
 - (2) For more information about mandatory briefings, refer to the *internal Mandatory Briefings - ITM Privacy Awareness Training site*.
- 10.5.1.7.7
(12-31-2020)
Records and Information Management (RIM)
- (1) Records and Information Management (RIM) Office within 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 American taxpayer. The Federal Records Act requires the IRS to efficiently manage all IRS records until final disposition.
 - (3) Refer to the IRM 1.15 series, Records and Information Management, Files Management, for more information.
- 10.5.1.7.8
(09-15-2023)
Disclosure
- (1) Disclosure, within PGLD's Governmental Liaison, Disclosure and Safeguards (GLDS), supports the Disclosure program. Disclosure safeguards confidential records, from the mailroom to the Commissioner's office. The word "sensitive" encompasses every type of SBU data from tax records to personal employee data.
 - (2) Tax returns and return information are SBU data. IRC 6103 provides the general rule that tax returns and return information are confidential information that we must not disclose except as provided 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 guidelines governing 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) Refer to the *internal Disclosure site*.
- (5) Refer to the external site for submitting a FOIA Request:
<https://www.irs.gov/privacy-disclosure/irs-freedom-of-information>

10.5.1.7.9
(09-15-2023)
**Digital Identity Risk
Assessment (DIRA)**

- (1) Digital Identity Risk Assessment (DIRA) is a joint effort between IT Cybersecurity and Online Services to establish a framework for establishing authentication risk consistently across online web-based electronic transactions.
- (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 component parts, referred to as *Identity Assurance Level (IAL)*, *Authenticator Assurance Level (AAL)*, and *Federation Assurance Level (FAL)*.

Note: The DIRA process applies to online web-based transactions.

- (3) For information about risk assessments of online services, contact **IT Cyber CPO DIRA*.

10.5.1.7.10
(09-15-2023)
**Enterprise Life Cycle
(ELC) and One Solution
Delivery Life Cycle
(OneSDLC)**

- (1) The IT Enterprise Life Cycle (ELC) office manages the ELC and OneSDLC program.
- (2) The IRS ELC and OneSDLC are the methodologies by which the IRS manages project activities through established standard processes.
 - a. The Enterprise Architecture (EA) is an integral component of ELC compliance process particularly from Milestone 1 through Milestone 4a.
 - b. The ELC and OneSLDC provide the direction, processes, tools, and assets necessary to accomplish business change in a consistent and repeatable manner as they implement the EA.
 - c. OneSDLC is replacing the ELC. Instead of milestones, OneSDLC has 3 stages: Allocation, Readiness, and Execution.
- (3) For more information about the ELC, refer to IRM 2.16.1, Enterprise Life Cycle (ELC), ELC Guidance. For more information about OneSDLC, refer to IRM 2.31.1, Lifecycle Management - One Solution Delivery Life Cycle Guidance, or the *OneSDLC site*.

10.5.1.7.11
(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. All IRS personnel should contact GL prior to 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 gov-

ernmental 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, LBI 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, Communications and Liaison, Office of Governmental Liaison, Governmental Liaison Operations.
- (4) For more information about GL's programs, refer to the *internal GL site*.

10.5.1.7.12
(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, Office of Governmental Liaison, Data Exchange Program, and IRM 11.3.39, Disclosure of Official Information, Computer Matching and Privacy Protection Act.

10.5.1.7.13
(12-31-2020)
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 *internal IA sites*.

10.5.1.7.13.1
(09-15-2023)
**Electronic Signature
(e-Signature) Program**

- (1) 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 the *internal e-Signature site*. For any further questions, contact the *PGLD IA eSignature mailbox.
- (3) For detailed information on the e-signature program, refer to IRM 10.10.1, Identity Assurance, IRS Electronic Signature (e-Signature) Program.

10.5.1.7.13.2
(09-15-2023)
**Non-Digital
Authentication Risk
Assessment (NDARA)**

- (1) The Identity Assurance IRM 10.10.2, Authentication Risk Assessments in Non-Digital Channels, details this policy, owned by PGLD's IA 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 (see IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)) for electronic interactions. 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*

10.5.1.7.14
(09-15-2023)
IT Security

- (1) IT Security Policy, under Cybersecurity Threat Response and Remediation, Oversight & Strategic Management, supports IT security policy and implementation.
- (2) IT security and privacy issues go together. Information Technology security policy describes how to protect IT environments, while privacy policy describes how to protect individuals' information in those IT environments. Information Technology 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.
- (4) For more information about the Cybersecurity program, refer to the *internal Cybersecurity site*.

10.5.1.7.15
(09-15-2023)
Incident Management (IM)

- (1) Incident Management (IM), within PGLD's PPC, is dedicated to assisting taxpayers and personnel potentially impacted by IRS breaches by working quickly and thoroughly to investigate 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/breach to the manager and the appropriate organizations based on what was lost or disclosed.
- (4) Anyone discovering a breach must report the breach to the appropriate organizations.
- (5) For more information about how to report an incident/breach, refer to IRM 10.5.4, Privacy and Information Protection, Incident Management Program, or the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets site*.

10.5.1.7.16
(09-24-2020)
Pseudonym

- (1) Incident Management (IM), within PGLD's PPC, manages the IRS Pseudonym program.
- (2) Under certain conditions (protection of personal safety, adequate justification, pre-approval, etc.), the Pseudonym program provides for the use of pseudonyms by IRS employees. The IRS Incident Management operation helps employees protect the privacy of these pseudonyms.
- (3) Refer to IRM 10.5.7, Use of Pseudonyms by IRS Employees

- 10.5.1.7.17
(09-15-2023)
Safeguards
- (1) The Safeguards program and staff are responsible for ensuring 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 the *internal Safeguards site*.
 - (3) Refer to IRM 11.3.36, Safeguard Review Program.
- 10.5.1.7.18
(09-24-2020)
Social Security Number Elimination and Reduction (SSN ER)
- (1) Information Protection Projects (IPP), under PGLD's Identity and Records Protection (IRP), administers 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]
 - (3) For more information, refer to the *internal SSN ER site* or email *PGLD SSN Reduction.
- 10.5.1.7.18.1
(03-23-2018)
Acceptable Use of SSNs
- (1) Use of SSNs is acceptable when any of these options mandates such use:
 - Law/statute.
 - Executive orders.
 - Federal regulations.
 - Business need (e.g., the inability to alter systems, processes, or forms due to costs or unacceptable level of risk).
- 10.5.1.7.18.2
(07-08-2021)
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 determine whether SSN use is justifiable and necessary:
 - a. **Apply the SSN Necessary-Use Criteria**
Based on the definition of the necessary and/or acceptable use of SSNs:
 1. Provide an accurate and complete citation of what authority (legislative mandate, regulation, or executive order) justifies SSN usage.
 2. 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/collection
 - Conversion/use and display
 - Migration/transmission
 - Storage
 - Deletion/disposal
 3. Determine whether the SSN is a critical component 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.

Note: Step c contains procedures for completing and submitting Form 14132, Social Security Number Retention Justification for Forms, Letters, Notices, and Systems.
 - b. **Identify SSN Elimination and Reduction Solutions**
After identifying potential areas to reduce or eliminate SSN use, collabo-

rate with business unit stakeholders to explore and identify feasible short- and long-term mitigation solutions, and submit a written mitigation plan to IPP by email to *PGLD SSN Reduction.

c. **Develop a Mitigation Strategy for Existing Inventories**

Whether SSN use is determined to be necessary or unnecessary, develop and provide to PGLD/IPP a mitigation strategy for existing forms, notices, and letters inventories on Form 14132.

d. **When Creating New Forms, Notices, Letters, and Systems**

Business/system owners must practice due diligence when creating new forms, notices, letters, and systems to ensure they apply the necessary-use criteria.

For New...	The Process Is...
Forms	W&I 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, the Privacy Notices section.)
Notices/ Letters	The Office of Taxpayer Correspondence will ask owners to consider use of SSNs on all newly created notices/letters. These questions and answers will become part of the interview file and maintained 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 demonstrate that program/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 maintain the justification for SSN usage.

e. **Manage Inventory**

PGLD will use completed Forms 14132 to manage the SSN ER Program and report progress to Treasury and IRS executive leadership.

f. **Reassess Periodically**

Once every three years, business/systems owners must reassess any forms, notices, letters, or systems to determine if conditions have changed that allow for the elimination or masking the SSN on their products. Business/system owners must inform the SSN ER Program of updated statuses on each product.

10.5.1.7.19
(12-31-2020)
**SBU Data Use for
Non-Production
Environments**

- (1) Privacy Compliance and Assurance (PCA), within PGLD's PPC, 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 appropriate. 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*.

10.5.1.7.20
(09-15-2023)
**Quick Response (QR)
Codes**

- (1) Office of Taxpayer Correspondence in Media and Publishing manages the Quick Response (QR) codes for the IRS.
- (2) The program objective is to provide taxpayers with targeted, prompt guidance and outreach. Using IRS-created QR codes allows the IRS to minimize data collection (to collect only necessary data), to protect taxpayer privacy and civil rights, to reduce costs, and to ensure that the experience instills trust and consistency.
- (3) Refer to IRM 1.17.7, Use of the Official IRS Seal, IRS Logo, Program Logos and Internal Logos.

10.5.1.8
(09-15-2023)
**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. This section addresses all the controls relevant to privacy and applies to security and privacy authorization to operate.

Note: This section is for technical management officials developing and supporting IT systems, including Management, Senior Management/Executives, System Owners, System Developers, and Authorizing Officials.

- (2) 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 particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. Controls are selected and implemented by the organization in order to satisfy the system requirements. Controls can include administrative, technical, and physical aspects.
 - For federal information security and privacy policies, the term *requirement* is generally used to refer to information security and privacy obligations imposed on organizations.
and
The term *requirement* can also be used in a broader sense to refer to an expression of stakeholder protection needs for a particular system or organization. Stakeholder protection needs and the corresponding security and privacy requirements may be derived from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments).
 - The term *processing* collectively refers to “the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal” of PII.
- (3) This section’s naming structure follows the pattern shown here in this example:
**AC-3(14) Access Control -- Access Enforcement - Individual Access [P]
{Org}**

- **AC-3:** The 2-letter control abbreviation NIST uses for the control family with a dash and the control number
- **(14):** *This part is used only for the controls that are control enhancements (CEs); the CE number is in parentheses and merged with the control enhancement number (IRM 10.8.1 uses this convention)*
- **Access Control:** Control family name
- **Access Enforcement:** Control name
- **Individual Access:** Control enhancement name, if applicable
- **[P]** for privacy or **[J]** for joint security and privacy:
 - If a control is privacy-owned [P], the language of the control is here in this IRM.
 - If a control is jointly owned by security and privacy [J], the language of the control is in IRM 10.8.1. IRM 10.8.1 includes the IT security roles and responsibilities and refers to this IRM for the privacy roles and responsibilities.
 - The security [S] controls are in IRM 10.8.1.
- **{Org}** for organizational common control (OCC), **{Sys}** for system control, or **{Hybrid}** for hybrid OCC and system control.
- All joint and privacy controls are for Low, Moderate, and High systems.

Note: Privacy is about the data, not the system.

(4) How this IRM shows the control information:

- a. If joint, this IRM shows the IRM 10.8.1 section name; if privacy, then this IRM repeats the NIST control language (ending with the attribution [NIST SP 800-53]), with *any IRS organization-defined parameters italicized*.

Note: If the control differs from the NIST baseline, then this note will explain how it differs and who requires it. When the IRS PGLD/ Cyber [NIST SP 800-53] Rev 5 Collaboration Working Group indicates a change from the NIST baseline for IRS assessment, the Note refers to IRS Collaboration.

- b. If the control is not a “-1” (“Policy and Procedures”) control, the next paragraph is the privacy concern.
- c. The **Implementation guidance** paragraph summarizes how the IRS implements that control to address that concern.

Note: Every information collection is unique and requires consideration; when questions arise needing consultation, contact **Privacy*.

- d. References to policy related to the control in this IRM follow in the pattern: IRM section number, section name. (Sections referenced include all of its subsections. Sometimes specific subsections are listed in parentheses to emphasize them.)
- e. If the privacy roles and responsibilities reside with a different privacy program, references to the appropriate IRM or program documentation follow with names of specific sections following, when applicable. The pattern is Type-of-publication Reference#: Section Name. Multiple section names are separated by commas. When multiple section names include commas, they are separated with semicolons. If the reference says, “throughout and specifically,” the specific section is only a starting point.

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

10.5.1.8.1

(09-15-2023)

**AC-1 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, see the AC-1 Access Control section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Control access to those authenticated and authorized individuals with a need to know.
 - b. Allow access by individuals to their own information as allowed by law.
- (3) In this IRM, PGLD policies on access control policy and procedures control include, but are not limited to, the sections:
 - a. IRM 10.5.1.1.1, Purpose of the Program
 - b. IRM 10.5.1.1.2, Audience
 - c. IRM 10.5.1.2, Key Privacy Definitions [Sensitive But Unclassified (SBU) Data, Unauthorized Access of SBU Data, Privacy Act Information, Authentication, Authorization, Need To Know]
 - d. IRM 10.5.1.3.2, IRS Privacy Principles (Strict Confidentiality; Security; Access, Correction, and Redress)
 - e. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (including Employees/Personnel, System Owners, System Developers, Personnel Engaged in Procurement Activities)
 - f. IRM 10.5.1.5.1, Clean Desk Policy
 - g. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data (including Limiting Sharing of SBU Data)
 - h. IRM 10.5.1.6.2, Encryption (including External, Internal)
 - i. IRM 10.5.1.6.3, Computers and Mobile Computing Devices
 - j. IRM 10.5.1.6.6, Storage
 - k. IRM 10.5.1.6.8.2, Emails to Other External Stakeholders
 - l. IRM 10.5.1.6.10, Disposition and Destruction
 - m. IRM 10.5.1.6.15, Contractors
 - n. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
 - o. IRM 10.5.1.6.18, Data on Collaborative Technology and Systems (including Shared Calendar; Online Meetings; Shared IRS Storage (OneDrive, SharePoint, Teams, and Other IRS Collaborative Sites), Cloud Computing)
 - p. IRM 10.5.1.6.19, Training
 - q. IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)
 - r. IRM 10.5.1.7.11, Governmental Liaison (GL)
- (4) PGLD and IRS also address access control policy and procedures control in the following:
 - a. IRM 10.5.2: Program Scope and Objectives, Background, Qualifying Questionnaire (QQ) for PCLIA, Surveys Accessed by Links, Determining SharePoint PIA Requirement, Shared Storage PIAs
 - b. IRM 10.5.4: Program Scope and Objectives; Responsibilities; Authority; Terms; Reporting Losses, Thefts and Disclosures (Intentional Unauthorized Disclosures of Tax Information; Inadvertent Accesses of Tax Information); PGLD/Incident Management Intake, Risk Assessment and Notification (OMB Major Incidents, PGLD/Incident Management Risk Assessment)
 - c. IRM 10.5.6: Content of a SORN; Privacy Act Requests for Non-Tax Records

- d. IRM 10.5.5: throughout, and specifically Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements
- e. IRM 10.5.8: Security controls applicable to non-production data
- f. IRM 11.3.22: Access by IRS Employees
- g. IRM 1.2.1: Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights
- h. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.1.1
(09-15-2023)

**AC-3(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 privacy concerns are that individuals have access to the information that the IRS has on them, as governed by the applicable laws and regulations.
- (3) **Implementation guidance:** The IRS implements this control by publishing SORNs and PCLIA's and handling requests for information under the Privacy Act, IRC, and FOIA.
- (4) In this IRM, PGLD policies on the individual access control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2.9, Access, Correction, and Redress
 - b. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
- (5) PGLD and IRS also address the individual access control in the following:
 - a. IRM 10.5.2: PCLIA's on IRS.gov
 - b. IRM 10.5.6: Privacy Act SORNs; Privacy Act Requests for Non-Tax Records
 - c. IRM 11.3.13: throughout, and specifically FOIA and Routine Established Agency Procedures for other types of requests (including tax information)
 - d. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.2
(09-15-2023)

**AT-1 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, see the AT-1 Awareness and Training Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Remain aware of and trained on the proper treatment of SBU data, including PII and tax information based on their roles.
 - b. Track such training records.
- (3) In this IRM, PGLD policies on the awareness and training policy and procedures control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles (Privacy Awareness and Training)

- b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (including Employees/Personnel, Management, Senior Management/Executives, System Owners, Personnel Engaged in Procurement Activities)
 - c. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data (including Limiting Sharing of SBU Data)
 - d. IRM 10.5.1.6.10.6, Contractors
 - e. IRM 10.5.1.7.1, IRS Privacy Council
 - f. IRM 10.5.1.7.6, Mandatory Briefings
- (4) PGLD and IRS also address the awareness and training policy and procedures control in the following:
- a. IRM 10.5.2: Program Scope and Objectives, PCLIA Roles and Responsibilities
 - b. IRM 10.5.4: Program Scope and Objectives, Responsibilities, Awareness Training and Education
 - c. IRM 10.5.5: throughout, and specifically Servicewide Roles and Responsibilities for Administering the IRS UNAX Program, Manager UNAX Responsibilities, IRP UNAX Program Team Roles and Responsibilities
 - d. IRM 10.5.6: Privacy Act Training
 - e. IRM 10.5.8: Security controls applicable to non-production data
 - f. IRM 11.3.1: Roles and Responsibilities
 - g. IRM 1.15.1: Responsibilities of the IRS Records Officer, Responsibilities of the RIM Records Specialist
 - h. IRM 1.1.27: Roles and Responsibilities
 - i. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.2.1
(09-15-2023)

AT-2 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, see the AT-2 Literacy Training and Awareness section of IRM 10.8.1.
- (2) The privacy concerns are 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) In this IRM, PGLD policies on the literacy training and awareness control include, but are not limited to, the sections listed in the AT-1 references, IRM 10.5.1.8.2.
- (5) PGLD and IRS also address the literacy training and awareness control in the sections listed in the AT-1 references, IRM 10.5.1.8.2

10.5.1.8.2.2
(09-15-2023)

AT-3 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, see the AT-3 Role-Based Training section of IRM 10.8.1.
- (2) The privacy concerns are 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) In this IRM, PGLD policies on the role-based training control include, but are not limited to, the sections listed in the AT-1 references, IRM 10.5.1.8.2.
- (5) PGLD and IRS also address the role-based training control in the sections listed in the AT-1 references, IRM 10.5.1.8.2

10.5.1.8.2.3
(09-15-2023)

AT-3(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 privacy concerns are that all personnel processing PII understand how to protect privacy.
- (3) **Implementation guidance:** The IRS implements this control by requiring annual mandatory role-based briefings on security and privacy.
- (4) In this IRM, PGLD policies on the processing personally identifiable information control include, but are not limited to, the sections listed in the AT-1 references, IRM 10.5.1.8.2.
- (5) PGLD and IRS also address the processing personally identifiable information control in the sections listed in the AT-1 references, IRM 10.5.1.8.2

10.5.1.8.2.4
(09-15-2023)

AT-4 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, see the AT-4 Training Records section of IRM 10.8.1.
- (2) The privacy concerns are tracking the training records to ensure that all personnel are current on privacy training and awareness.
- (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) In this IRM, PGLD policies on the training records control include, but are not limited to, the sections listed in the AT-1 references, IRM 10.5.1.8.2.
- (5) PGLD and IRS also address the training records control in the sections listed in the AT-1 references, IRM 10.5.1.8.2.

10.5.1.8.3
(09-15-2023)

AU-1 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, see the AU-1 Audit and Accountability Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having 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, PGLD policies on the audit and accountability policy and procedures control include, but are not limited to, the sections:

- a. IRM 10.5.1.2.8, Need To Know
 - b. IRM 10.5.1.3.2, IRS Privacy Principles (Accountability; Minimizing Collection, Use, Retention, and Disclosure; Strict Confidentiality)
 - c. IRM 10.5.1.6.15, Contractors
 - d. IRM 10.5.1.6.14.3, Monitoring Individuals
 - e. IRM 10.5.1.6.18.4, Cloud Computing
- (4) PGLD and IRS also address the audit and accountability policy and procedures control in the following:
- a. IRM 10.5.2: Determining SharePoint PIA Requirement, Authority for BPRAs
 - b. IRM 10.5.5: throughout, and specifically Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
 - c. IRM 10.5.8: Security controls applicable to non-production data
 - d. IRM 1.2.1: Mission of the Service, Taxpayer Privacy Rights
 - e. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.3.1
(09-15-2023)
AU-2 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, see the AU-2 Event Logging section of IRM 10.8.1.
- (2) The privacy concerns are that logging events (audit logs, audit trails, event logs, etc.) can reveal information about individuals.
- (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) In this IRM, PGLD policies on the event logging control include, but are not limited to, the section IRM 10.5.1.6.14.3, Monitoring Individuals.
- (5) PGLD and IRS also address the event logging control in the following:
- a. IRM 10.5.2: Determining SharePoint PIA Requirement
 - b. IRM 10.5.5: Background
 - c. IRM 10.5.8: Security controls applicable to non-production data
 - d. IRM 1.15.6: Creation, Use, and Maintenance of Unstructured Electronic Data
 - e. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.3.2
(09-15-2023)
AU-3(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 privacy concerns are that “Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.”
- (3) **Implementation guidance:** The IRS implements this control by requiring systems limit PII in audit records to the minimum necessary.
- (4) In this IRM, PGLD policies on the limit personally identifiable information elements control include, but are not limited to, the sections:
- a. IRM 10.5.1.2.8, Need To Know

- b. IRM 10.5.1.3.2, IRS Privacy Principles (Minimizing Collection, Use, Retention, and Disclosure; Strict Confidentiality)
- c. IRM 10.5.1.6.14.3, Monitoring Individuals

(5) PGLD and IRS also address the limit personally identifiable information elements control in the following:

- a. IRM 10.5.5: throughout, and specifically Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
- b. IRM 10.5.8: Security controls applicable to non-production data
- c. IRM 1.2.1: Mission of the Service, Taxpayer Privacy Rights
- d. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.3.3
(09-15-2023)

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, see the AU-11 Audit Record Retention section of IRM 10.8.1.
- (2) The privacy concerns are that the IRS retains audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions for the proper period to maintain transparency.
- (3) **Implementation guidance:** The IRS implements this control by adhering to the IRS records managements requirements.
- (4) In this IRM, PGLD policies on the audit record retention control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2.3, Minimizing Collection, Use, Retention, and Disclosure
 - b. IRM 10.5.1.4.4, Systems Owners
 - c. IRM 10.5.1.7.7, Records and Information Management (RIM)
- (5) PGLD and IRS also address the audit record retention control in the following:
 - a. IRM 1.15.6: Retention and Disposition of Electronic Records
 - b. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.4
(09-15-2023)

CA-1 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, see the CA-1 Assessment Authorization and Monitoring Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having 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, PGLD policies on the assessment authorization and monitoring policy and procedures control include, but are not limited to, the sections:

- a. IRM 10.5.1.2, Key Privacy Definitions [Sensitive But Unclassified (SBU) Data, Personally Identifiable Information (PII), Federal Tax Information (FTI)]
 - b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (including System Owners, Authorizing Officials)
 - c. IRM 10.5.1.3.1, Privacy Controls
 - d. IRM 10.5.1.3.2, IRS Privacy Principles
 - e. IRM 10.5.1.6.18.4, Cloud Computing
 - f. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - g. IRM 10.5.1.7.3, Business PII Risk Assessment (BPRA)
 - h. IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)
 - i. IRM 10.5.1.7.13.2, Non-Digital Authentication Risk Assessment (NDARA)
- (4) PGLD and IRS also address the assessment authorization and monitoring policy and procedures control in the following:
- a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA), PCLIA Roles and Responsibilities, Major Change Determination (MCD) for PCLIA, Business PII Risk Assessment (BPRA), Responsibilities, BPRA Roles and Responsibilities
 - b. IRM 10.5.4: PGLD/Incident Management Risk Assessment
 - c. IRM 10.5.5: Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
 - d. IRM 10.5.6: OMB Privacy Act Guidance; Agency Review Requirements
 - e. IRM 10.5.8: Security controls applicable to non-production data
 - f. *Pub 5499, IRS Privacy Program Plan*
 - g. Document 13347, Data Breach Response Playbook
 - h. Document 13347-A, IRS Data Breach Response Plan

10.5.1.8.4.1
(09-15-2023)
**CA-2 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, see the CA-2 Control Assessments section of IRM 10.8.1.
- (2) The privacy concerns are to ensure 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.
- (4) In this IRM, PGLD policies on the control assessments control include, but are not limited to, the sections listed in the CA-1 references, IRM 10.5.1.8.4.
- (5) PGLD and IRS also address the control assessments control in the sections listed in the CA-1 references, IRM 10.5.1.8.4.

10.5.1.8.4.2
(09-15-2023)
**CA-5 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, see the CA-5 Plan of Action and Milestones section of IRM 10.8.1.
- (2) The privacy concerns are to monitor privacy on POA&Ms.
- (3) **Implementation guidance:** The IRS implements this control by requiring System Owners monitor and address privacy risks identified on the PCLIA in a POA&M.

- (4) In this IRM, PGLD policies on the plan of action and milestones control include, but are not limited to, the section IRM 10.5.1.4.4, System Owners.
- (5) PGLD and IRS also address the plan of action and milestones control in IRM 10.5.2: Roles and Responsibilities.
- 10.5.1.8.4.3
(09-15-2023)
CA-6 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, see the CA-6 Authorization section of IRM 10.8.1.
- (2) The privacy concerns are to address privacy requirements before authorization to operate.
- (3) **Implementation guidance:** The IRS implements this control by including privacy in the ELC (specifically PCLIAAs) or OneSDLC (across the life cycle).
- (4) In this IRM, PGLD policies on the authorization control include, but are not limited to, the sections listed in the CA-1 references, IRM 10.5.1.8.4.
- (5) PGLD and IRS also address the authorization control in the sections listed in the CA-1 references, IRM 10.5.1.8.4.
- 10.5.1.8.4.4
(09-15-2023)
CA-7 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, see the CA-7 Continuous Monitoring section of IRM 10.8.1.
- (2) The privacy concerns are to maintain ongoing awareness of developing vulnerabilities.
- (3) **Implementation guidance:** The IRS implements this control by following the *Pub 5499, IRS Privacy Program Plan*.
- (4) In this IRM, PGLD policies on the continuous monitoring control include, but are not limited to, the sections listed in the CA-1 references, IRM 10.5.1.8.4.
- (5) PGLD and IRS also address the continuous monitoring control in the sections listed in the CA-1 references, IRM 10.5.1.8.4.
- 10.5.1.8.4.5
(09-15-2023)
CA-7(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, see the CA-7 Continuous Monitoring section of IRM 10.8.1.
- (2) The privacy concerns are to monitor and address privacy risks.
- (3) **Implementation guidance:** The IRS implements this control by monitoring risks identified in PCLIAAs, BPRAs, POA&Ms, and other assessment practices.
- (4) In this IRM, PGLD policies on the risk monitoring control include, but are not limited to, the sections listed in the CA-1 references, IRM 10.5.1.8.4.
- (5) PGLD and IRS also address the risk monitoring control in the sections listed in the CA-1 references, IRM 10.5.1.8.4.

10.5.1.8.5
(09-15-2023)
**CM-1 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, see the CM-1 Configuration Management Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having 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, PGLD policies on the configuration management policy and procedures control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2, Key Privacy Definitions
 - b. IRM 10.5.1.3, Key Privacy Concepts
 - c. IRM 10.5.1.4, IRS-Wide Roles and Responsibilities
 - d. IRM 10.5.1.6.2, Encryption
 - e. IRM 10.5.1.6.9.7, Electronic and Online [Other Forms of Transmission]
- (4) PGLD and IRS also address the configuration management policy and procedures control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA), Major Change Determination (MCD) for PCLIA
 - b. IRM 10.5.6: SORN Reports
 - c. IRM 10.5.8: Security controls applicable to non-production data

10.5.1.8.5.1
(09-15-2023)
**CM-4 Configuration
Management -- Impact
Analyses [J] {Sys}**

- (1) This is a joint security and privacy control about impact analyses. For the full text of the control, see the CM-4 Impact Analyses section of IRM 10.8.1.
- (2) The privacy concerns are 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) In this IRM, PGLD policies on the impact analyses control include, but are not limited to, the sections listed in the CA-1 references.
- (5) PGLD and IRS also address the impact analyses control in the sections listed in the CA-1 references.

10.5.1.8.6
(09-15-2023)
**IR-1 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, see the IR-1 Incident Response Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Provide mandatory incident management training on how to identify and respond to a breach.

- b. Testing the breach response plan.
 - c. Coordinate incident handling with IM, Cyber, CSIRC, and others as needed.
 - d. Report, track, document, and plan for incidents and response.
 - e. Supply a support resource for incident response.
- (3) In this IRM, PGLD policies on the incident response policy and procedures control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles (Strict Confidentiality, Security)
 - b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Employees/ Personnel, Management, Personnel Engaged in Procurement Activities)
 - c. IRM 10.5.1.6.4, Data Loss
 - d. IRM 10.5.1.7.15, Incident Management (IM)
- (4) PGLD and IRS also address the incident response policy and procedures control in the following:
 - a. IRM 10.5.4 throughout
 - b. Document 13347, Data Breach Response Playbook
 - c. Document 13347-A, IRS Data Breach Response Plan
 - d. *If/Then Guide for Reporting Incidents and Breaches*

10.5.1.8.6.1
(09-15-2023)
**IR-2 Incident Response
-- Incident Response
Training [J] {Org}**

- (1) This is a joint security and privacy control about incident response training. For the full text of the control, see the IR-2 Incident Response Training section of IRM 10.8.1.
- (2) The privacy concerns are that IRS personnel need to know who to call or how to recognize an incident or a 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) In this IRM, PGLD policies on the incident response training control include, but are not limited to, the sections listed in the IR-1 references, IRM 10.5.1.8.6.
- (5) PGLD and IRS also address the incident response training control in the following:
 - a. IRM 10.5.4: Awareness Training and Education
 - b. *If/Then Guide for Reporting Incidents and Breaches*

10.5.1.8.6.2
(09-15-2023)
**IR-2(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 privacy concerns are that IRS personnel need to know who to call or how to recognize a breach involving PII.
- (3) **Implementation guidance:** The IRS implements this control by providing mandatory training that includes information on how to identify and respond to a breach. The training includes links to how to respond to a breach.
- (4) In this IRM, PGLD policies on the breach control include, but are not limited to, the sections listed in the IR-1 references, IRM 10.5.1.8.6.
- (5) PGLD and IRS also address the breach control in the following:

- a. IRM 10.5.4: Awareness Training and Education; Reporting Losses, Thefts and Disclosures

10.5.1.8.6.3
(09-15-2023)

**IR-3 Incident Response
-- Incident Response
Testing [J] {Org}**

- (1) This is a joint security and privacy control about incident response testing. For the full text of the control, see the IR-3 Incident Response Testing section of IRM 10.8.1.
- (2) The privacy concerns are that IRS personnel test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies.
- (3) **Implementation guidance:** The IRS implements this control by testing the breach response plan annually in compliance with OMB M-17-12.
- (4) In this IRM, PGLD policies on the incident response testing control include, but are not limited to, the sections listed in the IR-1 references, IRM 10.5.1.8.6.
- (5) PGLD and IRS also address the incident response testing control in the following:
 - a. IRM 10.5.4: Responsibilities
 - b. Document 13347, Data Breach Response Playbook: Section 4.2, Tabletop Exercises: Testing the Plan
 - c. Document 13347-A, IRS Data Breach Response Plan: Section 10.1, Tabletop Exercises

10.5.1.8.6.4
(09-15-2023)

**IR-4 Incident Response
-- Incident Handling [J]
{Org}**

- (1) This is a joint security and privacy control about incident handling. For the full text of the control, see the IR-4 Incident Handling section of IRM 10.8.1.
- (2) The privacy concerns are the IRS has the capability to handle all types of incidents consistent with the incident response plan.
- (3) **Implementation guidance:** The IRS implements this control by coordinating incident handling with IM, Cyber, CSIRC, and other business units as needed.
- (4) In this IRM, PGLD policies on the incident handling control include, but are not limited to, the sections listed in the IR-1 references, IRM 10.5.1.8.6.
- (5) PGLD and IRS also address the incident handling control in the following:
 - a. IRM 10.5.4: Responsibilities
 - b. Document 13347, Data Breach Response Playbook: Section 5

10.5.1.8.6.5
(09-15-2023)

**IR-5 Incident Response
-- Incident Monitoring [J]
{Org}**

- (1) This is a joint security and privacy control about incident monitoring. For the full text of the control, see the IR-5 Incident Monitoring section of IRM 10.8.1.
- (2) The privacy concerns are the IRS tracks and documents incidents.
- (3) **Implementation guidance:** The IRS implements this control by using a tracking system.
- (4) In this IRM, PGLD policies on the incident monitoring control include, but are not limited to, the sections listed in the IR-1 references, IRM 10.5.1.8.6.
- (5) PGLD and IRS also address the incident monitoring control in the following:
 - a. IRM 10.5.4: PGLD/Incident Management Intake

- b. Document 13347, Data Breach Response Playbook: Section 2.0, Breach Response Team (BRT); Section 3.0, Data Breach Response Process
- c. 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
(09-15-2023)

**IR-6 Incident Response
-- Incident Reporting [J]
{Org}**

- (1) This is a joint security and privacy control about incident reporting. For the full text of the control, see the IR-6 Incident Reporting section of IRM 10.8.1.
- (2) The privacy concerns are that the IRS reports incidents or breaches.
- (3) **Implementation guidance:** The IRS implements this control by requiring all personnel report when an incident or breach occurs.
- (4) In this IRM, PGLD policies on the incident reporting control include, but are not limited to, the sections listed in the IR-1 references, IRM 10.5.1.8.6.
- (5) PGLD and IRS also address the incident reporting control in the following:
 - a. IRM 10.5.4: Reporting Losses, Thefts and Disclosures; PGLD/Incident Management Intake

10.5.1.8.6.7
(09-15-2023)

**IR-7 Incident Response
-- Incident Response
Assistance [J] {Org}**

- (1) This is a joint security and privacy control about incident response assistance. For the full text of the control, see the IR-7 Incident Response Assistance section of IRM 10.8.1.
- (2) The privacy concerns are that IRS provides a support resource that offers advice and assistance to personnel for the handling and reporting of incidents.
- (3) **Implementation guidance:** The IRS implements this control by offering a hotline.
- (4) In this IRM, PGLD policies on the incident response assistance control include, but are not limited to, the sections listed in the IR-1 references, IRM 10.5.1.8.6.
- (5) PGLD and IRS also address the incident response assistance control in the following:
 - a. IRM 10.5.4: Responsibilities; Related Resources; Inadvertent Unauthorized Disclosures and Losses or Thefts of IT Assets, BYOD Assets and Hardcopy Records/Documents; PGLD/Incident Management Intake

10.5.1.8.6.8
(09-15-2023)

**IR-8 Incident Response
-- Incident Response
Plan [J] {Org}**

- (1) This is a joint security and privacy control about incident response plan. For the full text of the control, see the IR-8 Incident Response Plan section of IRM 10.8.1.
- (2) The privacy concerns are that IRS develop and implement a coordinated approach to incident 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) In this IRM, PGLD policies on the incident response plan control include, but are not limited to, the sections listed in the IR-1 references, IRM 10.5.1.8.6.

- (5) PGLD and IRS also address the incident response plan control in the following:
- a. IRM 10.5.4: Responsibilities
 - b. Document 13347, Data Breach Response Playbook
 - c. Document 13347-A, IRS Data Breach Response Plan
- 10.5.1.8.6.9
(09-15-2023)
IR-8(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. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
 - b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms;
 - c. Identification of applicable privacy requirements.
- [NIST SP 800-53]
- (2) The privacy concerns are that IRS develop and implement a coordinated approach to incidents.
- (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) In this IRM, PGLD policies on the breaches control include, but are not limited to, the sections listed in the IR-1 references, IRM 10.5.1.8.6.
- (5) PGLD and IRS also address the breaches control in the following:
- a. IRM 10.5.4: Reporting Losses, Thefts and Disclosures; PGLD/Incident Management Risk Assessment
 - b. Document 13347, Data Breach Response Playbook
 - c. Document 13347-A, IRS Data Breach Response Plan
- 10.5.1.8.7
(09-15-2023)
MP-1 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, see the MP-1 Media Protection Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
- a. Prevent the unauthorized disclosure of information when reusing or releasing media for disposal.
 - b. Follow records management and disposition and destruction requirements.
- (3) In this IRM, PGLD policies on the media protection policy and procedures control include, but are not limited to, the sections:
- a. IRM 10.5.1.2, Key Privacy Definitions [Sensitive But Unclassified (SBU) Data, Personally Identifiable Information (PII), Federal Tax Information (FTI), Unauthorized Access of SBU Data, Privacy Act Information, Need To Know]

- b. IRM 10.5.1.3.2, IRS Privacy Principles (Strict Confidentiality, Security)
- c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities
- d. IRM 10.5.1.5.1, Clean Desk Policy
- e. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data (including Limiting Sharing of SBU Data)
- f. IRM 10.5.1.6.2, Encryption (including External, Internal)
- g. IRM 10.5.1.6.3, Computers and Mobile Computing Devices
- h. IRM 10.5.1.6.5, Marking
- i. IRM 10.5.1.6.6, Storage
- j. IRM 10.5.1.6.9, Other Forms of Transmission
- k. IRM 10.5.1.6.10, Disposition and Destruction
- l. IRM 10.5.1.6.15, Contractors

- (4) PGLD and IRS also address the media protection policy and procedures control in the following:

- a. IRM 10.5.6: Requirements of the Privacy Act
- b. IRM 1.15.6: Security of Electronic Records, Retention and Disposition of Electronic Records
- c. IRM 11.3.12: throughout, and specifically Official Use Only

10.5.1.8.7.1
(09-15-2023)

**MP-6 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, see the MP-6 Media Sanitization section of IRM 10.8.1.
- (2) The privacy concerns are 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 compliance with media sanitization requirements.
- (4) In this IRM, PGLD policies on the media sanitization control include, but are not limited to, the sections:
 - a. IRM 10.5.1.6.10, Disposition and Destruction
 - b. IRM 10.5.1.7.7, Records and Information Management (RIM)
- (5) PGLD and IRS also address the media sanitization control in the following:
 - a. IRM 10.5.6: Requirements of the Privacy Act
 - b. IRM 1.15.6: Retention and Disposition of Electronic Records

10.5.1.8.8
(09-15-2023)

**PE-1 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, see the PE-1 Physical and Environmental Protection Policy and Procedures section of IRM 10.8.1.

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 by having 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, PGLD policies on the physical and environmental protection policy and procedures control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2.11, High Security Items
 - b. IRM 10.5.1.3.2, IRS Privacy Principles (Purpose Limitation; Minimizing Collection, Use, Retention, and Disclosure; Security)
 - c. IRM 10.5.1.5.1, Clean Desk Policy
- (4) PGLD and IRS also address the physical and environmental protection policy and procedures control in the following:
 - a. IRM 10.5.6: Requirements of the Privacy Act

10.5.1.8.8.1
(09-15-2023)

PE-8(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 privacy concerns are that limiting PII elements in visitor access records when such information is not needed for operational purposes helps reduce the level of privacy risk.
- (3) **Implementation guidance:** The IRS implements this control by collecting only minimum necessary information in visitor access records.
- (4) In this IRM, PGLD policies on the limit personally identifiable information elements control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles (Purpose Limitation; Minimizing Collection, Use, Retention, and Disclosure; Security)
- (5) PGLD and IRS also address the limit personally identifiable elements control in the following:
 - a. IRM 10.5.6: Requirements of the Privacy Act

10.5.1.8.9
(09-15-2023)

PL-1 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, see the PL-1 Planning Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having 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, PGLD policies on the planning policy and procedures control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3, Key Privacy Concepts (Privacy Controls, IRS Privacy Principles)
 - b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (System Owners, System Developers, Authorizing Officials)
 - c. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
 - d. IRM 10.5.1.6.17, Social Media

- e. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
- f. IRM 10.5.1.7.10, Enterprise Life Cycle (ELC) and One Solution Delivery Life Cycle (OneSDLC)
- g. IRM 10.5.1.7.14, IT Security

(4) PGLD and IRS also address the planning policy and procedures control in the following:

- a. IRM 10.5.2: throughout, and specifically Responsibilities, PCLIA Roles and Responsibilities, System PCLIA's, Determining SharePoint PIA Requirement, FISMA Reporting
- b. IRM 10.5.6: Privacy Act SORNs
- c. IRM 10.5.8: Security controls applicable to non-production data
- d. IRM 1.15.1: Responsibilities of the IRS Records Officer
- e. IRM 1.15.6: Creation, Use, and Maintenance of Structured Electronic Data; Security of Electronic Records

10.5.1.8.9.1
(09-15-2023)

PL-2 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, see the PL-2 System Security and Privacy Plan section of IRM 10.8.1.
- (2) The privacy concerns are that privacy needs to be incorporated into the system development lifecycle.
- (3) **Implementation guidance:** The IRS implements this control by following the ELC or OneSDLC, completing the PCLIA process, and including privacy requirements in the system security and privacy plans.
- (4) In this IRM, PGLD policies on the system security and privacy plan control include, but are not limited to, the sections listed in the PL-1 references, IRM 10.5.1.8.9.
- (5) PGLD and IRS also address the system security and privacy plan control in the sections listed in the PL-1 references, IRM 10.5.1.8.9.

10.5.1.8.9.2
(09-15-2023)

PL-4 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, see the PL-4 Rules of Behavior section of IRM 10.8.1.
- (2) The privacy concerns are that all personnel with access to PII understand and follow the IRS *internal Rules of Behavior*.
- (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) In this IRM, PGLD policies on the rules of behavior control include, but are not limited to, the section IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities.
- (5) PGLD and IRS also address the rules of behavior control in the following:
 - a. IRM 10.5.5: IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program
 - b. IRM 11.3.1: Disclosure Code, Authority and Procedure (CAP)
 - c. Document 12011, IRS Ethics Handbook

- 10.5.1.8.9.3
(09-15-2023)
PL-4(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, see the PL-4 Rules of Behavior section of IRM 10.8.1.
 - (2) The privacy concerns are that all personnel with access to PII understand and follow the *internal Social Media Guidelines site* and the IRS *internal Rules of Behavior*.
 - (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) In this IRM, PGLD policies on the social media and external site/application usage restrictions control include, but are not limited to, the sections:
 - a. IRM 10.5.1.6.11.2, Location Services
 - b. IRM 10.5.1.6.17, Social Media
 - (5) PGLD and IRS also address the social media and external site/application usage restrictions control in the following:
 - a. IRM 10.5.2: Social Media PCLIA
 - b. IRM 11.1.3: Media Responsibilities
 - c. IRM 11.3.21: Use of Social Networking and Other Internet Sites by IRS Employees for Compliance Research or for Other Purpose
 - d. IRM 1.15.6: Use of Social Media
 - e. Document 12011, IRS Ethics Handbook
- 10.5.1.8.9.4
(09-15-2023)
PL-8 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, see the PL-8 Security and Privacy Architecture section of IRM 10.8.1.
 - (2) The privacy concerns are that privacy needs to be incorporated into the system development lifecycle.
 - (3) **Implementation guidance:** The IRS implements this control by following the ELC or OneSDLC, completing the PCLIA process, and including privacy requirements in the system security and privacy architecture.
 - (4) In this IRM, PGLD policies on the security and privacy architecture control include, but are not limited to, the sections listed in the PL-1 references, IRM 10.5.1.8.9.
 - (5) PGLD and IRS also address the security and privacy architecture control in the sections listed in the PL-1 references, IRM 10.5.1.8.9.
- 10.5.1.8.9.5
(09-15-2023)
PL-9 Planning -- Central Management [J] {Org}
- (1) This is a joint security and privacy control about central management. For the full text of the control, see the PL-9 Central Management section of IRM 10.8.1.
Note: This control differs from the NIST baseline where it is privacy, but joint per IRS Collaboration requirements.
 - (2) The privacy concerns are to support 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) In this IRM, PGLD policies on the central management control include, but are not limited to, the sections listed in the PL-1 references, IRM 10.5.1.8.9.
- (5) PGLD and IRS also address the central management control in the sections listed in the PL-1 references, IRM 10.5.1.8.9.

10.5.1.8.10
(07-08-2021)
**PM-1 Program
Management**

- (1) The PM-1 is a security-only [S] control in IRM 10.8.1. Privacy program plans are addressed separately in PM-18.

10.5.1.8.10.1
(09-15-2023)
**PM-3 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, see the PM-3 Information Security and Privacy Resources section of IRM 10.8.1.
- (2) The privacy concerns are that privacy programs have 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 ensure their programs and policies allocate sufficient resources to comply with IRS privacy policies and procedures.
- (4) In this IRM, PGLD policies on the information security and privacy resources control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles (Accountability)
 - b. IRM 10.5.1.4, IRS-Wide Roles and Responsibilities (Senior Management/Executives)
- (5) PGLD and IRS also address the information security and privacy resources control in the following:
 - a. IRM 1.1.27: Roles and Responsibilities, Program and Planning Support
 - b. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.10.2
(09-15-2023)
**PM-4 Program
Management -- Plan of
Action and Milestones
[J] {Org}**

- (1) This is a joint security and privacy control about plan of action and milestones. For the full text of the control, see the PM-4 Plan of Action and Milestones section of IRM 10.8.1.
- (2) The privacy concerns are to reduce 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) In this IRM, PGLD policies on the plan of action and milestones control include, but are not limited to, the section, IRM 10.5.1.4.4, System Owners.
- (5) PGLD and IRS also address the plan of action and milestones control in IRM 10.5.2: Roles and Responsibilities.

10.5.1.8.10.3

(09-15-2023)

PM-5(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 privacy concerns are the IRS uses this inventory to ensure that systems only process the PII for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein.
- (3) **Implementation guidance:** The IRS implements this control by reviewing the PCLIA inventory at least annually.
- (4) In this IRM, PGLD policies on the inventory of personally identifiable information control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles (Purpose Limitation, Security)
- (5) PGLD and IRS also address the inventory of personally identifiable information control in the following:
 - a. IRM 10.5.2: throughout, and specifically, Privacy Reporting
 - b. IRM 10.5.6: SORN Responsibilities

10.5.1.8.10.4

(09-15-2023)

PM-6 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, see the PM-6 Measures of Performance section of IRM 10.8.1.
- (2) The privacy concerns are to measure 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) In this IRM, PGLD policies on the measures of performance control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles (Purpose Limitation, Security)
- (5) PGLD and IRS also address the measures of performance control in the following:
 - a. IRM 10.5.2: FISMA Reporting
 - b. IRM 10.5.4: Program Management and Review; Timeliness of the Data Breach Notification
 - c. IRM 11.3.13: FOIA Reporting
 - d. IRM 11.3.39: Annual Matching Activity Review and Report

10.5.1.8.10.5

(09-15-2023)

PM-7 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, see the PM-7 Enterprise Architecture section of IRM 10.8.1.

- (2) The privacy concerns are to ensure that privacy considerations are addressed throughout the system development life cycle and are explicitly related to the organization's mission and business processes.
- (3) **Implementation guidance:** The IRS implements this control by requiring compliance with Enterprise Architecture's standards.
- (4) In this IRM, PGLD policies on the enterprise architecture control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3, Key Privacy Concepts
 - b. IRM 10.5.1.7.10, Enterprise Life Cycle (ELC) and One Solution Delivery Life Cycle (OneSDLC)
- (5) PGLD and IRS also address the enterprise architecture control in the following:
 - a. IRM 10.5.2: Background, System PCLIA's, Reconciliation with As-Built Architecture (ABA)

10.5.1.8.10.6
(09-15-2023)
**PM-8 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, see the PM-8 Critical Infrastructure Plan section of IRM 10.8.1.
- (2) The privacy concerns are the IRS address 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) In this IRM, PGLD policies on the critical infrastructure plan control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2.1, Privacy Lifecycle
 - b. IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data
- (5) PGLD and IRS also address the critical infrastructure plan control in the following:
 - a. IRM 10.5.2: PCLIA's Relevance to Privacy Compliance
 - b. IRM 10.6.1: Responsibilities

10.5.1.8.10.7
(09-15-2023)
**PM-9 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, see the PM-9 Risk Management Strategy section of IRM 10.8.1.
- (2) The privacy concerns are that the IRS manage privacy risk to individuals resulting from the authorized processing of PII.
- (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) In this IRM, PGLD policies on the risk management strategy control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2, Key Privacy Definitions [Sensitive But Unclassified (SBU) Data, Personally Identifiable Information (PII), Federal Tax Information (FTI)]
 - b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (including System Owners, Authorizing Officials)
 - c. IRM 10.5.1.3.1, Privacy Controls
 - d. IRM 10.5.1.3.2, IRS Privacy Principles (Accountability, Minimizing Collection, Use, Retention, and Disclosure, Strict Confidentiality)
 - e. IRM 10.5.1.6.1.1, Deciding Risk Levels for SBU Data
 - f. IRM 10.5.1.6.18.4, Cloud Computing
 - g. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - h. IRM 10.5.1.7.3, Business PII Risk Assessment (BPRA)
 - i. IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)
 - j. IRM 10.5.1.7.13.2, Non-Digital Authentication Risk Assessment (NDARA)
- (5) PGLD and IRS also address the risk management strategy control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA), Major Change Determination (MCD) for PCLIA, Business PII Risk Assessment (BPRA), Responsibilities, BPRA Roles and Responsibilities
 - b. IRM 10.5.4: PGLD/Incident Management Risk Assessment
 - c. IRM 10.5.5: Servicewide Roles and Responsibilities for Administering the IRS UNAX Program,
 - d. IRM 10.5.6: OMB Privacy Act Guidance; Agency Review Requirements
 - e. IRM 10.5.8: Security controls applicable to non-production data
 - f. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.10.8
(09-15-2023)
**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, see the PM-10 Authorization Process section of IRM 10.8.1.
- (2) The privacy concerns are to address privacy requirements before authorization to operate.
- (3) **Implementation guidance:** The IRS implements this control by including privacy in the ELC (specifically PCLIA) or OneSDLC (across the life cycle).
- (4) In this IRM, PGLD policies on the authorization process control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2, Key Privacy Definitions [Sensitive But Unclassified (SBU) Data, Personally Identifiable Information (PII), Federal Tax Information (FTI)]
 - b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (including System Owners, Authorizing Officials)
 - c. IRM 10.5.1.3.1, Privacy Controls
 - d. IRM 10.5.1.3.2, IRS Privacy Principles
 - e. IRM 10.5.1.6.18.4, Cloud Computing
 - f. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - g. IRM 10.5.1.7.3, Business PII Risk Assessment (BPRA)
 - h. IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)
 - i. IRM 10.5.1.7.13.2, Non-Digital Authentication Risk Assessment (NDARA)

- (5) PGLD and IRS also address the authorization process control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA), Major Change Determination (MCD) for PCLIA, Business PII Risk Assessment (BPRA), Responsibilities, BPRA Roles and Responsibilities
 - b. IRM 10.5.4: PGLD/Incident Management Risk Assessment
 - c. IRM 10.5.5: Servicewide Roles and Responsibilities for Administering the IRS UNAX Program,
 - d. IRM 10.5.6: OMB Privacy Act Guidance; Agency Review Requirements
 - e. IRM 10.5.8: Security controls applicable to non-production data

10.5.1.8.10.9
(09-15-2023)
**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, see the PM-11 Mission and Business Process Definition section of IRM 10.8.1.
- (2) The privacy concerns are the IRS protects privacy in systems and safeguards privacy in everyday business processes supporting the IRS mission.
- (3) **Implementation guidance:** The IRS implements this control by requiring a privacy culture, wherein all personnel think about privacy before acting. The mission of the service requires the IRS safeguard privacy and protect privacy rights.
- (4) In this IRM, PGLD policies on the mission and business process definition control include, but are not limited to, the sections:
 - a. IRM 10.5.1.1.1, Purpose of the Program
 - b. IRM 10.5.1.3.2, IRS Privacy Principles
 - c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Employees/Personnel)
 - d. IRM 10.5.1.5, Privacy Culture [Privacy in Practice (PiP)]
- (5) PGLD and IRS also address the mission and business process definition control in the following:
 - a. IRM 10.5.2: Business PII Risk Assessment (BPRA)
 - b. IRM 10.5.6: Responsibilities, IRS Privacy Principles
 - c. IRM 11.3.1: Disclosure Code, Authority and Procedure (CAP)
 - d. IRM 1.1.27: Roles and Responsibilities
 - e. IRM 1.2.1: Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights

10.5.1.8.10.10
(09-15-2023)
**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, see the PM-13 Security and Privacy Workforce section of IRM 10.8.1.
- (2) The privacy concerns are the IRS develop and institutionalize the core privacy capabilities of personnel needed to protect organizational operations, assets, and individuals.
- (3) **Implementation guidance:** The IRS implements this control by defining and developing privacy training for PGLD and other privacy-minded personnel.
- (4) In this IRM, PGLD policies on the security and privacy workforce control include, but are not limited to, the sections:

- a. IRM 10.5.1.1.2, Audience
 - b. IRM 10.5.1.3.2, IRS Privacy Principles (Privacy Awareness and Training)
- (5) PGLD and IRS also address the security and privacy workforce control in the following:
- a. IRM 10.5.2: PCLIA Roles and Responsibilities
 - b. IRM 10.5.6: Privacy Act Training
 - c. IRM 1.1.27: Roles and Responsibilities
 - d. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.10.11

(09-15-2023)

**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, see the PM-14 Testing, Training, and Monitoring section of IRM 10.8.1.
- (2) The privacy concerns are that the IRS coordinates the training for personnel with access to PII and the testing of privacy controls.
- (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) In this IRM, PGLD policies on the testing, training, and monitoring control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles (Privacy Awareness and Training)
 - b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (including Employees/Personnel, Management, Senior Management/Executives, System Owners, Personnel Engaged in Procurement Activities)
 - c. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data
 - d. IRM 10.5.1.6.15, Contractors
 - e. IRM 10.5.1.7.6, Mandatory Briefings
- (5) PGLD and IRS also address the testing, training, and monitoring control in the following:
 - a. IRM 10.5.2: Program Scope and Objectives, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.4: Program Scope and Objectives; Responsibilities; Awareness Training and Education
 - c. IRM 10.5.5: throughout, and specifically Servicewide Roles and Responsibilities for Administering the IRS UNAX Program, Manager UNAX Responsibilities, IRP UNAX Program Team Roles and Responsibilities
 - d. IRM 10.5.6: Privacy Act Training
 - e. IRM 10.5.8: Security controls applicable to non-production data
 - f. IRM 11.3.1: Roles and Responsibilities
 - g. IRM 1.15.1: Responsibilities of the IRS Records Officer, Responsibilities of the RIM Records Specialist
 - h. IRM 1.1.27: Roles and Responsibilities
 - i. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.10.12
(09-15-2023)

**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, see the PM-15 Security and Privacy Groups and Associations section of IRM 10.8.1.
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 privacy concerns are the IRS maintain 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 Federal Privacy Council (FPC), International Association of Privacy Professionals (IAPP), etc.
- (4) In this IRM, PGLD policies on the security and privacy groups and associations control include, but are not limited to, the sections:
 - a. IRM 10.5.1.7.1, IRS Privacy Council
 - b. Exhibit 10.5.1-2, References
- (5) PGLD and IRS also address the security and privacy groups and associations control in the following:
 - a. IRM 1.1.27: Responsibilities
 - b. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.10.13
(09-15-2023)

**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, see the PM-17 Protecting Controlled Unclassified Information on External Systems section of IRM 10.8.1.
- (2) The privacy concerns are that all sensitive information is protected on external systems.
- (3) **Implementation guidance:** The IRS implements this control by requiring that contractors and external partners protect all SBU data (including PII and tax information), which means all IRS acquisitions and agreements contain proper language holding contractors and other service providers accountable for following federal and IRS privacy policies and procedures, such as privacy clauses 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.

Note: Once the IRS implements the CUI program, then these requirements will apply to all CUI.

- (4) In this IRM throughout, and specifically, PGLD policies on the protecting controlled unclassified information/SBU data on external systems control include, but are not limited to, the sections:
 - a. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Personnel Engaged in Procurement Activities)
 - b. IRM 10.5.1.6.15, Contractors
 - c. IRM 10.5.1.6.18.4, Cloud Computing
 - d. IRM 10.5.1.7.11, Governmental Liaison (GL)

e. IRM 10.5.1.7.17, Safeguards

- (5) PGLD and IRS also address the protecting controlled unclassified information/ SBU data on external systems control in the following:
- a. IRM 10.5.2: System PCLIA, Survey PCLIA, Shared Storage PIAs
 - b. IRM 10.5.4: Reporting Losses, Thefts, and Disclosures
 - c. IRM 10.5.5: throughout, and specifically Employee and Contractor UNAX Responsibilities
 - d. IRM 10.5.6: Responsibilities, Privacy Act Training, Privacy Act Contract Requirements
 - e. IRM 11.3.24: throughout, and specifically Requirements
 - f. IRM 11.3.36: throughout, and specifically Legal Requirements
 - g. IRM 11.4.1: throughout, and specifically Data Exchange Agreements
 - h. IRM 1.15.1: Responsibilities of all IRS Employees and Contractors
 - i. Document 13347, Data Breach Response Playbook: Section 5.4, External Third-Party Incidents
 - j. Document 13347-A, IRS Data Breach Response Plan: Section 2.5, Contractors

10.5.1.8.10.14
(09-15-2023)

**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 frequently 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 privacy concerns are that the IRS formally documents its privacy program.
- (4) **Implementation guidance:** The IRS implements this control by publishing the *Pub 5499, IRS Privacy Program Plan*.
- (5) In this IRM, PGLD policies on the Privacy Program Plan control include, but are not limited to, the sections:

- a. IRM 10.5.1.1, Program Scope and Objectives
- b. IRM 10.5.1.3.1, Privacy Controls

(6) PGLD and IRS also address the Privacy Program Plan control in the following:

- a. IRM 10.5.6: OMB Privacy Act Guidance
- b. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.10.15
(09-15-2023)

**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 privacy concerns are that the IRS has a senior official responsible for ensuring that IRS implements sound policies to protect SBU data (including PII and tax information).

- (3) **Implementation guidance:** The IRS implements this control by designating a Chief Privacy Officer (CPO); Treasury appoints the senior agency official for privacy (SAOP).

- (4) In this IRM, PGLD policies on the privacy program leadership role control include, but are not limited to, the sections:

- a. IRM 10.5.1.1.1, Purpose of the Program
- b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (including Senior Management/Executives)
- c. IRM 10.5.1.7.1, IRS Privacy Council

- (5) PGLD and IRS also address the privacy program leadership role control in the following:

- a. IRM 10.5.6: Responsibilities, OMB Privacy Act Guidance
- b. IRM 1.1.27: Roles and Responsibilities

10.5.1.8.10.16
(09-15-2023)

**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 privacy concerns are that people have a way to see privacy policies and contact the IRS regarding concerns.
- (3) **Implementation guidance:** The IRS implements this control by maintaining the IRS.gov Privacy Policy page <https://www.irs.gov/privacy> and giving the email privacy@treasury.gov.
- (4) In this IRM, PGLD policies on the dissemination of privacy program information control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles
 - b. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
- (5) PGLD and IRS also address the dissemination of privacy program information control in the following:
 - a. IRM 10.5.2: PCLIA's on IRS.gov
 - b. IRM 10.5.6: Privacy Act Publication and Reporting Requirements, Privacy Act Access and Amendment of Records
 - c. IRM 11.3.13: throughout, and specifically FOIA and Routine Established Agency Procedures for other types of requests (including tax information)

10.5.1.8.10.17
(09-15-2023)

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:
 - a. Are written in plain language and organized in a way that is easy to understand and navigate;
 - b. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and
 - c. 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 privacy concerns are the public can make an informed decision about sharing their information.
- (3) **Implementation guidance:** The IRS implements this control by both maintaining the IRS.gov Privacy Policy page <https://www.irs.gov/privacy> and a link to that page for all external facing online services.
- (4) In this IRM, PGLD policies on the privacy policies on websites, applications, and digital services control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2.4, Openness and Consent
 - b. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
- (5) PGLD and IRS also address the privacy policies on websites, applications, and digital services control in the following:
 - a. IRM 10.5.6: Online Privacy Policy Notices, Privacy Act Recordkeeping Restrictions

10.5.1.8.10.18
(09-15-2023)

**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 privacy concerns are to allow individuals to learn to whom their PII has been disclosed.
- (5) **Implementation guidance:** The IRS implements this control by requiring that employees authorized to make disclosures of non-tax Privacy Act records must account for such disclosures.
- (6) In this IRM, PGLD policies on the accounting of disclosures control include, but are not limited to, the section IRM 10.5.1.2.7, Privacy Act Information.
- (7) PGLD and IRS also address the accounting of disclosures control in the following:
 - a. IRM 10.5.6: Privacy Act Accounting for Disclosures
 - b. IRM 11.3.37: Accounting System

10.5.1.8.10.19
(09-15-2023)

**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 privacy concerns are to confirm the accuracy and relevance of PII throughout the information life cycle.
- (3) **Implementation guidance:** The IRS implements this control by requiring accuracy, completeness, and timeliness of PII to ensure fair treatment of all individuals. IRS personnel will collect information, to the greatest extent practical, directly from the individual to whom it relates.

- (4) In this IRM, PGLD policies on the personally identifiable information quality management control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2.1, Privacy Lifecycle
 - b. IRM 10.5.1.3.2, IRS Privacy Principles (Data Quality, Verification and Notification)
 - c. IRM 10.5.1.6.14, Civil Liberties
- (5) PGLD and IRS also address the personally identifiable information quality management control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.6: Program Scope and Objectives; Privacy Act General Provisions; Requirements of the Privacy Act; Privacy Act Recordkeeping Restrictions; Privacy Act Requirement to Maintain Accurate, Relevant, Timely, and Complete Records

10.5.1.8.10.20
(09-15-2023)
**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, see the PM-23 Data Governance Body section of IRM 10.8.1.

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 privacy concerns are that data, including PII, is effectively managed and maintained following applicable laws, executive orders, directives, regulations, policies, standards, and guidance.
- (3) **Implementation guidance:** The IRS implements this control by using the Cybersecurity & Privacy Management Level Governance Board to establish policies, procedures, and standards that facilitate data governance.
- (4) In this IRM, PGLD policies on the data governance body control include, but are not limited to, the sections:
 - a. IRM 10.5.1.1.6, Authority
 - b. IRM 10.5.1.7, Privacy-Related Programs

10.5.1.8.10.21
(09-15-2023)
**PM-24 Program
Management -- Data
Integrity Board [P] {Org}**

- (1) Establish a Data Integrity Board to:
 - a. Review proposals to conduct or participate in a matching program; and
 - b. 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 privacy concerns are the IRS monitor the agency's matching activities.
- (3) **Implementation guidance:** The IRS implements this control by having the CPO representing the IRS as a member of the Treasury Data Integrity Board.
- (4) In this IRM, PGLD policies on the data integrity board control include, but are not limited to, the sections:

- a. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data
- b. IRM 10.5.1.7.12, Data Services

(5) PGLD and IRS also address the data integrity board control in the following:

- a. IRM 10.5.6: Annual Matching Activity Review and Report
- b. IRM 11.3.39: throughout, and specifically Program Scope and Objectives

10.5.1.8.10.22
(09-15-2023)
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 if there is 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 privacy concerns are that the use of PII in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information.
- (6) **Implementation guidance:** The IRS implements this control by requiring the SBU Data Use process for non-production environments.
- (7) In this IRM, PGLD policies on the minimization of personally identifiable information used for testing, training, and research control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2.3, Minimizing Collection, Use, Retention, and Disclosure
 - b. IRM 10.5.1.7.19, SBU Data Use for Non-Production Environments
- (8) PGLD and IRS also address the minimization of personally identifiable information used for testing, training, and research control in the following:
 - a. IRM 10.5.8: throughout, and specifically all security controls applicable to non-production data

10.5.1.8.10.23
(09-15-2023)
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:
 - a. Mechanisms that are easy to use and readily accessible by the public;
 - b. All information necessary for successfully filing complaints;
 - c. Tracking mechanisms to ensure all complaints received are reviewed and addressed *within 20 business days*;
 - d. Acknowledgement of receipt of complaints, concerns, or questions from individuals *within 20 business days if the IRS will not be responding with the response within 20 days*; and

- e. Response to complaints, concerns, or questions from individuals *within 20 business days*. [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 privacy concerns are to respond to concerns that members of the public might have about their privacy.
- (3) **Implementation guidance:** The IRS implements this control by having a Privacy Complaints section on <https://www.irs.gov/privacy>.
- (4) In this IRM, PGLD policies on the complaint management control include, but are not limited to, the sections:
 - a. IRM 10.5.1.1.1, Purpose of the Program
 - b. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
- (5) PGLD and IRS also address the complaint management control in the following:
 - a. IRM 10.5.2: Section 803 Reporting
 - b. IRM 10.5.4: Caller Indicates He or She is a Victim of Identity Theft as a Result of an IRS Data Breach
 - c. IRM 10.5.6: Responsibilities, Section 803 Reports about Privacy Act Complaints
 - d. Pub 5499, IRS Privacy Program Plan

10.5.1.8.10.24
(09-15-2023)
**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:
 - a. *the appropriate oversight bodies in the Distribution Level(s) column* to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and
 - b. *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 privacy concerns are to promote accountability and transparency in organizational privacy operations.
- (4) **Implementation guidance:** The IRS implements this control by complying with established reporting activities.
- (5) In this IRM, PGLD policies on the privacy reporting control include, but are not limited to, the section IRM 10.5.1.7.4, Privacy Reporting.
- (6) PGLD and IRS also address the privacy reporting control in the following:
 - a. IRM 10.5.2: Reporting

- b. IRM 10.5.4: Measures and Reports; Inadvertent Unauthorized Disclosures and Losses or Thefts of IT Assets, BYOD Assets and Hardcopy Records/Documents [Treasury Government Security Operations Center (GSOC)]; High-Risk Data Breaches
- c. IRM 10.5.5: Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
- d. IRM 10.5.6: Privacy Act Publication and Reporting Requirements, including the section Privacy Act Reports
- e. IRM 11.3.13: FOIA Reporting
- f. IRM 11.3.37: Disclosure Accounting Report to the Joint Committee on Taxation (JCT)
- g. IRM 11.3.39: Matching Program Notice and Reporting Requirements
- h. *internal PGLD - All Internal and External Reports site*
- i. Document 13347-A, IRS Data Breach Response Plan: Section 11, Reports

10.5.1.8.10.25
(09-15-2023)

**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, see the PM-28 Risk Framing section of IRM 10.8.1.
- (2) The privacy concerns are that privacy considerations inform risk assessment, risk response, and risk monitoring activities.
- (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) In this IRM, PGLD policies on the risk framing control include, but are not limited to, the sections:
 - a. IRM 10.5.1.1.5, Background
 - b. IRM 10.5.1.3.2, IRS Privacy Principles
 - c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Management, Senior Management/Executives, System Owners, System Developers, Authorizing Officials, Personnel Engaged in Procurement Activities)
 - d. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII
 - e. IRM 10.5.1.6.1.1, Deciding Risk Levels for SBU Data and PII
 - f. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data and PII
 - g. IRM 10.5.1.6.8, Email
 - h. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - i. IRM 10.5.1.7.3, Business PII Risk Assessment (BPRA)
 - j. IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)
- (5) PGLD and IRS also address the risk framing control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA), Business PII Risk Assessment (BPRA)
 - b. IRM 10.5.4: Background; Responsibilities; PGLD/Incident Management Intake, Risk Assessment and Notification
 - c. IRM 10.5.8: Security controls applicable to non-production data
 - d. IRM 10.10.1: Oversight Procedure
 - e. *Pub 5499, IRS Privacy Program Plan*
 - f. Document 13347, Data Breach Response Playbook
 - g. Document 13347-A, IRS Data Breach Response Plan

10.5.1.8.10.26
(09-15-2023)
**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, see the PM-31 Continuous Monitoring Strategy section of IRM 10.8.1.
- (2) The privacy concerns are to conduct continuous monitoring to support organizational risk management decisions in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies.
- (3) **Implementation guidance:** The IRS implements this control by following the *Pub 5499, IRS Privacy Program Plan*.
- (4) In this IRM, PGLD policies on the continuous monitoring strategy control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2, Key Privacy Definitions [Sensitive But Unclassified (SBU) Data, Personally Identifiable Information (PII), Federal Tax Information (FTI)]
 - b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (including System Owners, Authorizing Officials)
 - c. IRM 10.5.1.3.1, Privacy Controls
 - d. IRM 10.5.1.3.2, IRS Privacy Principles
 - e. IRM 10.5.1.6.18.4, Cloud Computing
 - f. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - g. IRM 10.5.1.7.3, Business PII Risk Assessment (BPRA)
 - h. IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)
 - i. IRM 10.5.1.7.13.2, Non-Digital Authentication Risk Assessment (NDARA)
- (5) PGLD and IRS also address the continuous monitoring strategy control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA), Major Change Determination (MCD) for PCLIA, Business PII Risk Assessment (BPRA), Responsibilities, BPRA Roles and Responsibilities
 - b. IRM 10.5.4: PGLD/Incident Management Risk Assessment
 - c. IRM 10.5.5: Servicewide Roles and Responsibilities for Administering the IRS UNAX Program
 - d. IRM 10.5.6: OMB Privacy Act Guidance, Agency Review Requirements
 - e. IRM 10.5.8: Security controls applicable to non-production data
 - f. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.11
(09-15-2023)
**PS-1 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, see the PS-1 Personnel Security Policy and Procedures section of IRM 10.8.1

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 by having 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, PGLD policies on the personnel security policy and procedures control include, but are not limited to, the sections:

- a. IRM 10.5.1.1.2, Audience
- b. IRM 10.5.1.2.8, Need To Know
- c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities
- d. IRM 10.5.1.6.15, Contractors

- (4) PGLD and IRS also address the personnel security policy and procedures control in the following:

- a. IRM 10.5.5: IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program
- b. IRM 10.5.8: Security controls applicable to non-production data; throughout and specifically Requirement for Using SBU Data
- c. IRM 10.23 series, Personnel Security

10.5.1.8.11.1
(09-15-2023)

**PS-6 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, see the PS-6 Access Agreements section of IRM 10.8.1.
- (2) The privacy concerns are that all personnel with access to PII understand the IRS *internal Rules of Behavior* through access agreements.
- (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) In this IRM, PGLD policies on the access agreements control include, but are not limited to, the sections listed in the PS-1 references, IRM 10.5.1.8.11.
- (5) PGLD and IRS also address the access agreements control in the PS-1 references, IRM 10.5.1.8.11.

10.5.1.8.12
(09-15-2023)

**PT-1 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* 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* 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 by having policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
- Protect PII from unauthorized access, use, and disclosure.
 - Limit use of PII to the published authorities and purposes, with notice and consent as required by law.
 - 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, PGLD policies on the personally identifiable information processing and transparency policy and procedures control include all of IRM 10.5.1, but specifically the sections for transparency are:
- IRM 10.5.1.3.2, IRS Privacy Principles (Openness and Consent)
 - IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
- (6) PGLD and IRS also address the personally identifiable information processing and transparency policy and procedures control in the following:
- IRM 10.5.2: throughout, and specifically Program Scope and Objectives
 - IRM 10.5.4: throughout, and specifically Program Scope and Objectives
 - IRM 10.5.5: throughout, and specifically Program Scope and Objectives
 - IRM 10.5.6: throughout, and specifically Program Scope and Objectives
 - IRM 10.5.8: throughout, and specifically Program Scope and Objectives
 - IRM 11.3.1: throughout, and specifically Program Scope and Objectives
 - IRM 1.2.1: Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights

10.5.1.8.12.1
(09-15-2023)

**PT-2 Personally
Identifiable Information
Processing and
Transparency --
Authority to Process
Personally Identifiable
Information [P] {Org}**

- Determine and document the *Internal Revenue Code (IRC)*, *Privacy Act*, or other legal authority that permits the *processing* of personally identifiable information; and
- Restrict the *processing* of personally identifiable information to only that which is authorized. [NIST SP 800-53]
- The privacy concerns are that the IRS processes PII only for authorized purposes.
- 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 and requires consideration; when questions arise needing consultation, contact **Privacy*.

- (5) In this IRM, PGLD policies on the authority to process personally identifiable information control include, but are not limited to, the sections:

- a. IRM 10.5.1.1, Program Scope and Objectives (Authority), which lists primary authorities for processing PII
 - b. IRM 10.5.1.2, Key Privacy Definitions, including the Authorization section
 - c. IRM 10.5.1.3.2, IRS Privacy Principles
 - d. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities
 - e. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data
- (6) PGLD and IRS also address the authority to process personally identifiable information control in the following:
- a. IRM 10.5.2: Authority, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.5: throughout, and specifically Program Scope and Objectives
 - c. IRM 10.5.6: Authorities, Privacy Act General Provisions, Privacy Act Publication and Reporting Requirements, Privacy Act Notification Programs, Privacy Act Recordkeeping Restrictions
 - d. IRM 11.3.1: Disclosure Code, Authority and Procedure (CAP)
 - e. IRM 1.2.1: Policy Statement 1-1, Mission of the Service

10.5.1.8.12.2

(09-15-2023)

PT-3 Personally Identifiable Information Processing and Transparency -- Personally Identifiable Information Processing Purposes [P] {Org}

- (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 ensure that any changes are made in accordance with *this IRM and the IRS Privacy Principles*. [NIST SP 800-53]
- (5) The privacy concerns are that PII is processed only for identified purposes.
- (6) **Implementation guidance:** The IRS implements this control by requiring that personnel consult with PGLD to ensure any new purposes that arise from changes in processing are compatible with the purpose for which the information was collected. If the new purpose is not compatible, consult with PGLD to implement approaches following defined requirements to allow for the new processing, if appropriate. 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) In this IRM, PGLD policies on the personally identifiable information processing purposes control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2, Key Privacy Definitions
 - b. IRM 10.5.1.3.2, IRS Privacy Principles
 - c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities

- (8) PGLD and IRS also address the personally identifiable information processing purposes control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.6: Privacy Act General Provisions, Privacy Act Publication and Reporting Requirements, Privacy Act Notification Programs, Privacy Act Recordkeeping Restrictions
 - c. IRM 10.5.8: Privacy Authorities
 - d. IRM 11.3.1: Disclosure Code, Authority and Procedure (CAP)
 - e. IRM 1.2.1: Policy Statement 1-1, Mission of the Service

10.5.1.8.12.3
(09-15-2023)

**PT-4 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 privacy concerns are that individuals participate in making decisions about the processing of their information and provide consent as required by applicable laws.
- (3) **Implementation guidance:** The IRS implements this control by:
 - a. **Organization-level:** Implied consent. The fact that the entire 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) In this IRM, PGLD policies on the consent control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2.4, Openness and Consent
 - b. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
- (5) PGLD and IRS also address the consent control in the following:
 - a. IRM 10.5.2: External Surveys
 - b. IRM 10.5.6: Online Privacy Policy Notices, Privacy Act Recordkeeping Restrictions

10.5.1.8.12.4
(09-15-2023)

**PT-5 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 an IRS internet website or application, as well as on any page collecting substantial personal information from the public.*
 - 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 privacy notice when system-level website or application information collected is more specific than what IRS.gov privacy policy says.

[NIST SP 800-53]

- (2) The privacy concerns are that the IRS informs individuals about how their PII is processed.
- (3) **Implementation guidance:** The IRS implements this control by: providing notice with the required elements to individuals before collecting or processing information.
 - a. **Organization-level:** See IRM 10.5.1.6.16.1, IRS.gov Privacy Policy Notice.
 - b. **System-level:** See IRM 10.5.1.6.16.2, Online Data Collection Website or Application Privacy Policy Notice.
- (4) In this IRM, PGLD policies on the privacy notice control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2.4, Openness and Consent
 - b. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
- (5) PGLD and IRS also address the privacy notice control in the following:
 - a. IRM 10.5.2: External Surveys
 - b. IRM 10.5.6: throughout, and specifically Privacy Act Notification Programs [including Notice to Individuals Asked to Supply Information (Privacy Act Notice), Online Privacy Policy Notices]
 - c. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.12.5
(09-15-2023)

**PT-5(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 privacy concerns are that the IRS complies with the Privacy Act and informs individuals about how their PII is being processed.
- (3) **Implementation guidance:** The IRS implements this control by providing notice with the required elements to individuals before collecting or processing information.
- (4) In this IRM, PGLD policies on the Privacy Act statements control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2.4, Openness and Consent
 - b. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
- (5) PGLD and IRS also address the Privacy Act statement control in the following:
 - a. IRM 10.5.2: External Surveys
 - b. IRM 10.5.6: throughout, and specifically Privacy Act Notification Programs [including Notice to Individuals Asked to Supply Information (Privacy Act Notice), Online Privacy Policy Notices]
 - c. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.12.6
(09-15-2023)

**PT-6 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 privacy concerns are that IRS has the public-facing notice of the categories, authorities, purposes, and routine uses of the PII that the IRS collects.
- (3) **Implementation guidance:** The IRS implements this control by the publication and updating of SORNs following the SORN SOPs.
- (4) In this IRM, PGLD policies on the system of records notice control include, but are not limited to, the section IRM 10.5.1.2.7, Privacy Act Information.
- (5) PGLD and IRS also address the system of records notice control in the following:
 - a. IRM 10.5.2: PCLIA Roles and Responsibilities
 - b. IRM 10.5.6: throughout, and specifically Privacy Act Publication and Reporting Requirements
 - c. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.12.7
(09-15-2023)

**PT-6(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 year* 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 privacy concerns are that the routine uses control is compatible with the purpose for which the information was originally collected.
- (3) **Implementation guidance:** The IRS implements this control by reviewing PCLIAs and SORNs periodically on their appropriate cycles to ensure that routine uses continue to be compatible with the purpose for which the information was collected.
- (4) In this IRM, PGLD policies on the routine uses control include, but are not limited to, the section IRM 10.5.1.2.7, Privacy Act Information.
- (5) PGLD addresses the routine uses control in the section Agency Review Requirements in IRM 10.5.6.

- 10.5.1.8.12.8
(09-15-2023)
PT-6(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 privacy concerns are that the exemption rules control remain appropriate and necessary.
 - (3) **Implementation guidance:** The IRS implements this control by reviewing PCLIA's and SORNs periodically to ensure that exemptions remain appropriate.
 - (4) In this IRM, PGLD policies on the system of records notice control include, but are not limited to, the section IRM 10.5.1.2.7, Privacy Act Information.
 - (5) PGLD and IRS also address the exemption rules control in the following:
 - a. IRM 10.5.6: Agency Review Requirements
 - b. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*
- 10.5.1.8.12.9
(09-15-2023)
PT-7 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 privacy concerns are that some categories are particularly sensitive or raise privacy risks.
 - (3) **Implementation guidance:** The IRS implements this control by addressing different categories of PII based on sensitivity and context. Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary.
 - (4) In this IRM, PGLD policies on the specific categories of personally identifiable information control include all of IRM 10.5.1, and specifically IRM 10.5.1.2, Key Privacy Definitions.
 - (5) PGLD and IRS also address the specific categories of personally identifiable information control in the following:
 - a. IRM 10.5.2: Civil Liberties
 - b. IRM 10.5.5: throughout, and specifically IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program
 - c. IRM 10.5.6: throughout, and specifically Privacy Act Recordkeeping Restrictions
 - d. IRM 11.3 series: All discussion of tax information under the IRC
 - e. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*
- 10.5.1.8.12.10
(09-15-2023)
PT-7(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:
 - a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;
 - b. Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and

- c. Inform any individual who is asked to disclose his or her 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 privacy concerns are that social security numbers are particularly sensitive or raise privacy risks.
- (3) **Implementation guidance:** The IRS implements this control by:
 - a. Eliminating the unnecessary use of SSNs.
 - b. Not denying any right, benefit, or privilege. This does not apply when the SSN is required by federal statute, as it is in IRC 6109 and 5 USC.
 - c. Informing taxpayers and personnel that their SSN is mandatory under tax or employment law, and how we will use it.
- (4) In this IRM, PGLD policies on the social security numbers control include, but are not limited to, the sections:
 - a. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities
 - b. IRM 10.5.1.7.18, Social Security Number Elimination and Reduction (SSN ER)
- (5) PGLD and IRS also address the social security numbers control in the following:
 - a. IRM 10.5.5: throughout, and specifically IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program
 - b. IRM 10.5.6: Notice to Individuals Asked to Disclose Their Social Security Number
 - c. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.12.11
(09-15-2023)

**PT-7(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 privacy concerns are that the absence of First Amendment information from agency records helps to prevent selective treatment of persons on the basis of religion, opinion, or group membership.
- (3) **Implementation guidance:** The IRS implements this control by following the Privacy Act and not maintaining records of how individuals exercise their Constitutional First Amendment rights except as specifically authorized. Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary.
- (4) In this IRM, PGLD policies on the First Amendment information control include, but are not limited to, the section IRM 10.5.1.6.14.1, First Amendment.
- (5) PGLD and IRS also address the First Amendment information control in the following:
 - a. IRM 10.5.2: Civil Liberties
 - b. IRM 10.5.6: Privacy Act Recordkeeping Restrictions

c. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*10.5.1.8.12.12
(09-15-2023)**PT-8 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:
 - a. Obtain approval from the Data Integrity Board to conduct the matching program;
 - b. Develop and enter into a computer matching agreement;
 - c. Publish a matching notice in the Federal Register;
 - d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and
 - e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

[NIST SP 800-53]
- (2) The privacy concerns are that if an individual might be subject to an adverse action due to a matching program, that the individual has a way to identify the source of an adverse action.
- (3) **Implementation guidance:** The IRS implements this control by requiring computer matching agreements (CMAs) and Treasury Data Integrity Board approval.
- (4) In this IRM, PGLD policies on the computer matching agreements control include, but are not limited to, the sections:
 - a. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data
 - b. IRM 10.5.1.7.12, Data Services
- (5) PGLD and IRS also address the computer matching agreements control in the following:
 - a. IRM 10.5.6: Program Scope and Objectives
 - b. IRM 11.3.39: throughout, and specifically Program Scope and Objectives

10.5.1.8.13
(09-15-2023)**RA-1 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, see the RA-1 Risk Assessment Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having 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, PGLD policies on the risk assessment policy and procedures control include, but are not limited to, the sections:
 - a. IRM 10.5.1.1.5, Background
 - b. IRM 10.5.1.3.2, IRS Privacy Principles
 - c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Management, Senior Management/Executives, System Owners, System

Developers, Authorizing Officials, Personnel Engaged in Procurement Activities)

- d. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII
 - e. IRM 10.5.1.6.1.1, Deciding Risk Levels for SBU Data and PII
 - f. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data and PII
 - g. IRM 10.5.1.6.8, Email
 - h. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - i. IRM 10.5.1.7.3, Business PII Risk Assessment (BPRA)
 - j. IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)
- (4) PGLD and IRS also address the risk assessment policy and procedures control in the following:
- a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA), Business PII Risk Assessment (BPRA)
 - b. IRM 10.5.4: Background; Responsibilities; PGLD/Incident Management Intake, Risk Assessment and Notification
 - c. IRM 10.5.6: Agency Review Requirements
 - d. IRM 10.5.8: Security controls applicable to non-production data
 - e. IRM 10.10.1: Oversight Procedure
 - f. *Pub 5499, IRS Privacy Program Plan*
 - g. Document 13347, Data Breach Response Playbook
 - h. Document 13347-A, IRS Data Breach Response Plan

10.5.1.8.13.1
(09-15-2023)

**RA-3 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, see the RA-3 Risk Assessment section of IRM 10.8.1.
- (2) The privacy concerns are that privacy risks can be identified and addressed throughout the privacy lifecycle.
- (3) **Implementation guidance:** The IRS implements this control by conducting PCLIA's, BPRAs, and other risk assessment, response, and monitoring activities and sharing results with the CPO.
- (4) In this IRM, PGLD policies on the risk assessment control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles
 - b. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Management, Senior Management/Executives, System Owners, System Developers, Authorizing Officials, Personnel Engaged in Procurement Activities)
 - c. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII
 - d. IRM 10.5.1.6.1.1, Deciding Risk Levels for SBU Data and PII
 - e. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data and PII
 - f. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - g. IRM 10.5.1.7.3, Business PII Risk Assessment (BPRA)
 - h. IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)
 - i. IRM 10.5.1.7.15, Incident Management (IM)
- (5) PGLD and IRS also address the risk assessment control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA), Business PII Risk Assessment (BPRA)
 - b. IRM 10.5.4: Background; Responsibilities; PGLD/Incident Management Intake, Risk Assessment and Notification

- c. IRM 10.5.6: Agency Review Requirements
- d. IRM 10.5.8: Security controls applicable to non-production data
- e. IRM 10.10.1: Oversight Procedure
- f. *Pub 5499, IRS Privacy Program Plan*
- g. Document 13347, Data Breach Response Playbook
- h. Document 13347-A, IRS Data Breach Response Plan

10.5.1.8.13.2
(09-15-2023)

**RA-7 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, see the RA-7 Risk Response section of IRM 10.8.1.
- (2) The privacy concerns are that the IRS respond appropriately to risk to help protect privacy.
- (3) **Implementation guidance:** The IRS implements this control by avoiding or mitigating risks with strengthened controls, accepting risk with appropriate justification or rationale, and documenting actions taken.
- (4) In this IRM, PGLD policies on the risk response control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles
 - b. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII
 - c. IRM 10.5.1.6.1.1, Deciding Risk Levels for SBU Data and PII
 - d. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data and PII
 - e. IRM 10.5.1.7.15, Incident Management (IM)
- (5) PGLD and IRS also address the risk response control in the following:
 - a. IRM 10.5.2: PCLIA Roles and Responsibilities, BPRA Roles and Responsibilities
 - b. IRM 10.5.4: Background; Responsibilities; PGLD/Incident Management Intake, Risk Assessment and Notification
 - c. IRM 10.5.8: Security controls applicable to non-production data
 - d. IRM 10.10.1: Oversight Procedure
 - e. *Pub 5499, IRS Privacy Program Plan*
 - f. Document 13347, Data Breach Response Playbook
 - g. Document 13347-A, IRS Data Breach Response Plan

10.5.1.8.13.3
(09-15-2023)

**RA-8 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 privacy concerns are that IT systems that process PII be reviewed for privacy risks in compliance with the E-Government Act of 2002.

- (3) **Implementation guidance:** The IRS implements this control by requiring PCLIA's for IT systems that process PII.
- (4) In this IRM, PGLD policies on the privacy impact assessments control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2.3, Personally Identifiable Information (PII)
 - b. IRM 10.5.1.3.2, IRS Privacy Principles
 - c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Management, Senior Management/Executives, System Owners, System Developers, Authorizing Officials, Personnel Engaged in Procurement Activities)
 - d. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data and PII
 - e. IRM 10.5.1.6.1.1, Deciding Risk Levels for SBU Data and PII
 - f. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data and PII
 - g. IRM 10.5.1.6.14, Civil Liberties
 - h. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
- (5) PGLD and IRS also address the privacy impact assessments control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.6: Publication and Reporting Requirements Responsibilities
 - c. IRM 10.5.8: Requirements for Using SBU Data

10.5.1.8.14
(09-15-2023)
**SA-1 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, see the SA-1 System and Services Acquisition Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Fund and manage contracted information resources with PII.
 - b. Protect data throughout the privacy lifecycle.
 - c. Include privacy protections in contracts.
 - d. Engineer systems with minimal PII necessary.
 - e. Protect privacy in external system services.
 - f. Protect privacy in development and testing.
- (3) In this IRM, PGLD policies on the system and services acquisition policy and procedures control include, but are not limited to, the sections:
 - a. IRM 10.5.1.3.2, IRS Privacy Principles (Accountability)
 - b. IRM 10.5.1.4, IRS-Wide Roles and Responsibilities (Senior Management/Executives)
- (4) PGLD and IRS also address the system and services acquisition policy and procedures control in the following:
 - a. IRM 1.1.27: Roles and Responsibilities, Program and Planning Support
 - b. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.14.1
(09-15-2023)

**SA-2 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, see the SA-2 Allocation of Resources section of IRM 10.8.1.
- (2) The privacy concerns are that the IRS properly funds and manages contracted information resources, especially those that involve PII.
- (3) **Implementation guidance:** The IRS implements this control by requiring senior management and executives ensure their programs and policies meet this responsibility.
- (4) In this IRM, PGLD policies on the allocation of resources control include, but are not limited to, the sections:
 - a. IRM 10.5.1.1, Program Scope and Objectives
 - b. IRM 10.5.1.2.1, Privacy Lifecycle
 - c. IRM 10.5.1.3.2, IRS Privacy Principles (Accountability, Minimizing Collection, Use, Retention, and Disclosure)
 - d. IRS-Wide Privacy Roles and Responsibilities (Senior Management/ Executives, System Owners, System Developers, Personnel Engaged in Procurement Activities)
 - e. IRM 10.5.1.5, Privacy Culture
 - f. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data
 - g. IRM 10.5.1.6, Practical Privacy Policy (Computers and Mobile Computing Devices, Email, Contractors, Cloud Computing)
 - h. IRM 10.5.1.7.10, Enterprise Life Cycle (ELC) and One Solution Delivery Life Cycle (OneSDLC)
 - i. IRM 10.5.1.7.19, SBU Data Use for Non-Production Environments
- (5) PGLD and IRS also address the allocation of resources control in the following:
 - a. IRM 10.5.2: PCLIA's Relevance to Privacy Compliance, PCLIA Roles and Responsibilities
 - b. IRM 10.5.8: Security controls applicable to non-production data
 - c. IRM 1.15.1: Program Scope and Objectives
 - d. IRM 1.15.2: Stages of the Records Life Cycle
 - e. IRM 1.1.27: Roles and Responsibilities, Program and Planning Support
 - f. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.14.2
(09-15-2023)

**SA-3 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, see IRM 10.8.1, the SA-3 System Development Life Cycle section.
- (2) The privacy concerns are that sensitive data can be vulnerable across different life cycle stages, including the system development life cycle (SDLC) and the broader privacy lifecycle.
- (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) In this IRM, PGLD policies on the system development life cycle control include, but are not limited to, the sections:

- a. IRM 10.5.1.1, Program Scope and Objectives
- b. IRM 10.5.1.2.1, Privacy Lifecycle
- c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (System Owners, System Developers)
- d. IRM 10.5.1.5, Privacy Culture
- e. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data
- f. IRM 10.5.1.6.15, Contractors
- g. IRM 10.5.1.7.10, Enterprise Life Cycle (ELC) and One Solution Delivery Life Cycle (OneSDLC)

(5) PGLD and IRS also address the system development life cycle control in the following:

- a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA), PCLIA's Relevance to Privacy Compliance, PCLIA Roles and Responsibilities
- b. IRM 10.5.6: Relevant and Necessary Guidelines
- c. IRM 10.5.8: Security controls applicable to non-production data
- d. IRM 1.15.1: Program Scope and Objectives
- e. IRM 1.15.2: Stages of the Records Life Cycle
- f. *Pub 5499, IRS Privacy Program Plan*
- g. IRM 1.2.1: Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights

10.5.1.8.14.3
(09-15-2023)

SA-4 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, see the SA-4 Acquisition Process section of IRM 10.8.1.
- (2) The privacy concerns are that contract provisions incorporate privacy protections.
- (3) **Implementation guidance:** The IRS implements this control by requiring all IRS acquisitions and contract vehicles contain proper language holding contractors and other service providers accountable for following federal and IRS privacy policies and procedures, such as privacy clauses 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) In this IRM, PGLD policies on the acquisition process control include, but are not limited to, the sections listed in the SA-1 references, IRM 10.5.1.8.14.
- (5) PGLD and IRS also address the acquisition process control in the sections listed in the SA-1 references, IRM 10.5.1.8.14.

10.5.1.8.14.4
(09-15-2023)

SA-8(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 privacy concerns are the "relevant and necessary" requirement of the Privacy Act.
- (3) **Implementation guidance:** The IRS implements this control by collecting only information that is both relevant and necessary to accomplish the authorized purpose for which it is maintained.
- (4) In this IRM, PGLD policies on the minimization control include all of IRM 10.5.1, and specifically the principle in IRM 10.5.1.3.2.3, Minimizing Collection, Use, Retention, and Disclosure.

- (5) PGLD and IRS also address the minimization control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.6: Relevant and Necessary Guidelines
 - c. IRM 10.5.8: SBU Data Use Questionnaire
 - d. IRM 1.2.1: Policy Statement 1-1, Mission of the Service, Taxpayer Privacy Rights

10.5.1.8.14.5
(09-15-2023)
**SA-9 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, see the SA-9 External System Services section of IRM 10.8.1.
- (2) The privacy concerns are that the IRS's data is protected in external system services.
- (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 clauses 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) In this IRM, PGLD policies on the external system services control include, but are not limited to, the sections listed in the SA-1 references, IRM 10.5.1.8.14.
- (5) PGLD and IRS also address the external system services control in the sections listed in the SA-1 references, IRM 10.5.1.8.14.

10.5.1.8.14.6
(09-15-2023)
**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, see the SA-11 Developer Testing and Evaluation section of IRM 10.8.1.
- (2) The privacy concerns are that the systems and services acquired address privacy controls and that SBU data used in development and testing is also protected during the life cycle.
- (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) In this IRM, PGLD policies on the developer testing and evaluation control include, but are not limited to, the sections:
 - a. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Senior Management/Executives, System Owners, Personnel Engaged in Procurement Activities)
 - b. IRM 10.5.1.2.1, Privacy Lifecycle
 - c. IRM 10.5.1.3.2, IRS Privacy Principles
 - d. IRM 10.5.1.5, Privacy Culture
 - e. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data
 - f. IRM 10.5.1.6, Practical Privacy Policy (Computers and Mobile Computing Devices, Email, Contractors, Cloud Computing)
 - g. IRM 10.5.1.7.19, SBU Data Use for Non-Production Environments

- (5) PGLD and IRS also address the developer testing and evaluation control in the following:
- a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.6: Privacy Act Contract Requirements
 - c. IRM 10.5.8: Program Scope and Objectives, Requirements for Using SBU Data
 - d. IRM 11.3.24: Disclosure of Returns and Return Information to Vendors and Expert Services
 - e. *Pub 5499, IRS Privacy Program Plan*
 - f. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.15
(09-15-2023)

SC-1 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, see the SC-1 System and Communications Protection Policy and Procedures section of IRM 10.8.1.

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 by having 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, PGLD policies on the system and communications protection policy and procedures control include, but are not limited to, the sections:
- a. IRM 10.5.1.1.1, Purpose of the Program
 - b. IRM 10.5.1.1.2, Audience
 - c. IRM 10.5.1.2, Key Privacy Definitions [Sensitive But Unclassified (SBU) Data, Unauthorized Access of SBU Data, Privacy Act Information, Need To Know]
 - d. IRM 10.5.1.3.2, IRS Privacy Principles (Strict Confidentiality; Security; Access, Correction, and Redress)
 - e. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (including Employees/Personnel, System Owners, System Developers, Personnel Engaged in Procurement Activities)
 - f. IRM 10.5.1.5.1, Clean Desk Policy
 - g. IRM 10.5.1.6.1, Protecting and Safeguarding SBU Data (including Limiting Sharing of SBU Data)
 - h. IRM 10.5.1.6.2, Encryption (including External, Internal)
 - i. IRM 10.5.1.6.3, Computers and Mobile Computing Devices
 - j. IRM 10.5.1.6.8.2, Emails to Other External Stakeholders
 - k. IRM 10.5.1.6.10, Disposition and Destruction
 - l. IRM 10.5.1.6.15, Contractors
 - m. IRM 10.5.1.6.16, Online Data Collection and Privacy Notices
 - n. IRM 10.5.1.6.18, Data on Collaborative Technology and Systems (including Online Meetings; Shared IRS Storage (OneDrive, SharePoint, Teams, and Other IRS Collaborative Sites); Cloud Computing)
 - o. IRM 10.5.1.7.9, Digital Identity Risk Assessment (DIRA)
 - p. IRM 10.5.1.7.11, Governmental Liaison (GL)
- (4) PGLD and IRS also address the system and communications protection policy and procedures control in the following:

- a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
- b. IRM 10.5.4: Reporting Losses, Thefts and Disclosures
- c. IRM 10.5.6: Privacy Act General Provisions
- d. IRM 10.5.8: Security controls applicable to non-production data
- e. IRM 11.3.1: Program Scope and Objectives
- f. *Privacy & Civil Liberties Impact Assessment (PCLIA) Reference Guide*

10.5.1.8.15.1
(09-15-2023)

SC-7(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 privacy concerns are to ensure that PII is processed only following established privacy requirements.
- (3) **Implementation guidance:** The IRS implements this control by applying rules, monitoring, and documenting exceptions to processing rules.
- (4) In this IRM, PGLD policies on the boundary protection personally identifiable information control include, but are not limited to, the sections listed in the SC-1 references, IRM 10.5.1.8.15.
- (5) PGLD and IRS also address the boundary protection personally identifiable information control in the sections listed in the SC-1 references, IRM 10.5.1.8.15.

10.5.1.8.16
(09-15-2023)

SI-1 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, see the SI-1 System and Information Integrity Policy and Procedures section of IRM 10.8.1.
- (2) **Implementation guidance:** The IRS implements this control by having policy throughout this and all organizational IRMs that address this control family's concerns and require personnel to:
 - a. Protect data throughout the privacy lifecycle.
 - b. Minimize PII throughout the privacy lifecycle, including in testing, training, and research.
 - c. Enforce a retention period followed by proper disposal.
 - d. Follow the Privacy Act provisions for amendment and for accurate, relevant, timely, and complete records.
 - e. De-identify PII in datasets.
- (3) In this IRM, PGLD policies on the system and information integrity policy and procedures control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2, Key Privacy Definitions
 - b. IRM 10.5.1.3.2, IRS Privacy Principles
 - c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities
 - d. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data

- e. IRM 10.5.1.6.10, Disposition and Destruction
 - f. IRM 10.5.1.6.12, Telework
 - g. IRM 10.5.1.6.19, Training
 - h. IRM 10.5.1.6.20, Smart Devices
 - i. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - j. IRM 10.5.1.7.7, Records and Information Management (RIM)
- (4) PGLD and IRS also address the system and information integrity policy and procedures control in the following:
- a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.4: Retention and Disposition
 - c. IRM 10.5.6: Responsibilities; Requirements of the Privacy Act; OMB Privacy Act Guidance; Privacy Act Requirement to Maintain Accurate, Relevant, Timely, and Complete Records; Privacy Act Access and Amendment of Records
 - d. IRM 10.5.8: Security controls applicable to non-production data
 - e. IRM 11.3.1: Disclosure of Official Information; Introduction to Disclosure; Safeguarding and Disposing of Tax Returns, Return Information, and Other Confidential Records; Federal Tax Information Guidelines in IRS Training Programs; Records Disposition For Disclosure
 - f. IRM 11.3.11: Disclosure of Statistical Data
 - g. IRM 11.3.12: Protection of Return Information
 - h. IRM 11.3.22: Use of Tax Returns in Training Material
 - i. IRM 1.15.3: throughout, and specifically Destroying Records in the Custody of the IRS
 - j. IRM 1.11.2: Fictitious Identifying Information
 - k. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.16.1
(09-15-2023)

**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, see the SI-12 Information Management and Retention section of IRM 10.8.1.
- (2) The privacy concerns are that privacy risks can occur throughout the lifecycle and across any usage.
- (3) **Implementation guidance:** The IRS implements this control by protecting and minimizing SBU across the privacy lifecycle, to include minimizing, retaining safely, and disposing properly.
- (4) In this IRM, PGLD policies on the information management and retention control include, but are not limited to, the sections listed in the SI-1 references, IRM 10.5.1.8.16.
- (5) PGLD and IRS also address the information management and retention control in the sections listed in the SI-1 references, IRM 10.5.1.8.16.

- 10.5.1.8.16.2
(09-15-2023)
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 privacy concerns are that extraneous PII increases risk.
 - (3) **Implementation guidance:** The IRS implements this control by minimizing PII throughout the privacy lifecycle.
 - (4) In this IRM, PGLD policies on the limit personally identifiable information elements control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2, Key Privacy Definitions (Sensitive But Unclassified (SBU) Data, Personally Identifiable Information (PII), Federal Tax Information (FTI), Need To Know)
 - b. IRM 10.5.1.3.2, IRS Privacy Principles (Minimizing Collection, Use, Retention, and Disclosure)
 - c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Management, System Owners, System Developers, Personnel Engaged in Procurement Activities)
 - d. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data
 - e. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - (5) PGLD and IRS also address the limit personally identifiable information elements control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.6: OMB Privacy Act Guidance
 - c. IRM 10.5.8: Security controls applicable to non-production data
 - d. IRM 1.15.6: Managing Electronic Records
- 10.5.1.8.16.3
(09-15-2023)
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 fictitious, masked, or synthetic data*. [NIST SP 800-53]
 - (2) The privacy concerns are that other uses of data outside the production environment can increase privacy risks.
 - (3) **Implementation guidance:** The IRS implements this control by requiring the SBU Data Use process for non-production environments, adherence to the training fictitious data requirements, and the protections of research data.
 - (4) In this IRM, PGLD policies on the minimize personally identifiable information in testing, training, and research control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2, Key Privacy Definitions [Sensitive But Unclassified (SBU) Data, Personally Identifiable Information (PII), Federal Tax Information (FTI), Need To Know]
 - b. IRM 10.5.1.3.2, IRS Privacy Principles (Minimizing Collection, Use, Retention, and Disclosure)
 - c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Management, System Owners, System Developers, Personnel Engaged in Procurement Activities)
 - d. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data
 - e. IRM 10.5.1.6.19, Training

f. IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)

(5) PGLD and IRS also address the minimize personally identifiable information in testing, training, and research control in the following:

- a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
- b. IRM 10.5.6: OMB Privacy Act Guidance
- c. IRM 10.5.8: throughout, and specifically SBU Data Process
- d. IRM 11.3.1: Federal Tax Information Guidelines in IRS Training Programs
- e. IRM 11.3.22: Use of Tax Returns in Training Material
- f. IRM 1.11.2: Fictitious Identifying Information

10.5.1.8.16.4
(09-15-2023)

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*. [NIST SP 800-53]
- (2) The privacy concerns are that even older information can be sensitive.
- (3) **Implementation guidance:** The IRS implements this control by enforcing a retention period followed by proper disposal.
- (4) In this IRM, PGLD policies on the information disposal control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2, Key Privacy Definitions (Privacy Lifecycle)
 - b. IRM 10.5.1.3.2, IRS Privacy Principles (Minimizing Collection, Use, Retention, and Disclosure)
 - c. IRM 10.5.1.6.10, Disposition and Destruction
 - d. IRM 10.5.1.6.12, Telework
 - e. IRM 10.5.1.7.7, Records and Information Management (RIM)

- (5) PGLD and IRS also address the information disposal control in the following:
 - a. IRM 10.5.2: Privacy and Civil Liberties Impact Assessment (PCLIA)
 - b. IRM 10.5.4: Retention and Disposition
 - c. IRM 10.5.6: Responsibilities, Requirements of the Privacy Act, Privacy Act Contract Requirements
 - d. IRM 10.5.8: Security controls applicable to non-production data
 - e. IRM 11.3.1: Safeguarding and Disposing of Tax Returns, Return Information, and Other Confidential Records; Records Disposition For Disclosure
 - f. IRM 1.15.3: throughout, and specifically Destroying Records in the Custody of the IRS
 - g. IRM 1.15.6: Managing Electronic Records

10.5.1.8.16.5
(09-15-2023)

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 privacy concerns are that inaccurate PII 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.

- (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, the Statutory Exemption for Amendment of Tax Records section.

- (5) In this IRM, PGLD policies on the personally identifiable information quality operations control include, but are not limited to, the sections:

- a. IRM 10.5.1.2.7, Privacy Act Information
- b. IRM 10.5.1.3.2, IRS Privacy Principles (Data Quality; Access, Correction, and Redress)

- (6) PGLD and IRS also address the personally identifiable information quality operations control in the following:

- a. IRM 10.5.6: Privacy Act Requirement to Maintain Accurate, Relevant, Timely, and Complete Records; Privacy Act Access and Amendment of Records
- b. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.16.6
(09-15-2023)

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 privacy concerns are that inaccurate PII 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.

- (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, the Statutory Exemption for Amendment of Tax Records section.

- (4) In this IRM, PGLD policies on the individual requests control include, but are not limited to, the sections:

- a. IRM 10.5.1.2.7, Privacy Act Information
- b. IRM 10.5.1.3.2, IRS Privacy Principles (Data Quality; Access, Correction, and Redress)

- (5) PGLD and IRS also address the individual requests control in the following:

- a. IRM 10.5.6: Privacy Act Requirement to Maintain Accurate, Relevant, Timely, and Complete Records; Privacy Act Access and Amendment of Records
- b. *Pub 5499, IRS Privacy Program Plan*

10.5.1.8.16.7
(09-15-2023)
**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 privacy concerns are that many datasets contain PII, and certain elements or combinations of elements can re-identify individuals despite efforts to redact, mask, or truncate information.
- (4) **Implementation guidance:** The IRS implements this control by either removing PII elements described in this control or requiring the use of 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) In this IRM, PGLD policies on the de-identification control include, but are not limited to, the sections:
 - a. IRM 10.5.1.2.3, Personally Identifiable Information (PII)
 - b. IRM 10.5.1.2.4, Federal Tax Information (FTI)
 - c. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (System Owners, System Developers)
 - d. IRM 10.5.1.6.1.2, Limiting Sharing of SBU Data
 - e. IRM 10.5.1.6.19, Training
- (6) PGLD and IRS also address the de-identification control in the following:
 - a. IRM 10.5.2: Survey PCLIA
 - b. IRM 11.3.1: Disclosure of Official Information, Introduction to Disclosure
 - c. IRM 11.3.11: Disclosure of Statistical Data
 - d. IRM 11.3.12: Protection of Return Information
 - e. IRM 1.13.1: throughout, and specifically Statistical Reporting Overview
 - f. IRM 1.11.2: Fictitious Identifying Information

This Page Intentionally Left Blank

Exhibit 10.5.1-1 (09-15-2023)
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 therein, at an acceptable level of risk.(Refer to IRM 10.8.2 for more information.)
biometric technology	Biometric technology is a combination of the use of very sensitive personal information with automated analysis, frequently 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 previously available 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 for more information.
CNSI	Classified National Security Information
consent	Consent can be explicit (verbal or by other action) or implied (by continuing or inaction).
controls	From NIST SP 800-53 Rev 5, Section 2.1: <i>Controls</i> can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. Controls are selected and implemented by the organization in order to satisfy the system requirements. Controls can include administrative, technical, and physical aspects.
COR	Contracting Officer Representative
CPO	Chief Privacy Officer
critical areas	Refer to IRM 10.2.14, the Security Areas section.
CSP	Cloud Service Provider.
Data Owner	See Information Owner.

Exhibit 10.5.1-1 (Cont. 1) (09-15-2023)**Glossary and Acronyms**

Term	Definition or description
DIRA	Digital Identity Risk Assessment.
employee information	All employee information covered by the Privacy Act of 1974 (5 USC 552a, as amended). Examples include personnel, payroll, job applications, disciplinary actions, performance appraisals, drug tests, health exams, and evaluation data. Most employee information falls under the SBU data category called PII or Privacy information.
ELC	Enterprise Life Cycle; being replaced by One Solution Delivery Life Cycle (OneSDLC).
electronic mail message (email)	A record created or received on an electronic mail system including briefing notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message. Email is not encrypted by default and may be exchanged with recipients who are operating in a separate technology environment (domain), outside IRS control.
electronic media	Electronic media are electronic copy or devices containing 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/temporary employees 3. Interns 4. Detailees
EP	Employee Protection, within PGLD's Privacy Policy and Compliance (PPC).
Federal tax information (FTI)	Any return or return information as defined in IRC 6103(b). This includes any information obtained, received, or generated by IRS or any Treasury component with respect to determining liability, potential liability, or amount of liability under the IRC. FTI falls under the SBU data category called tax information or Tax. This IRM uses the term tax information to encompass all types of tax data.
FedRAMP	Federal Risk and Authorization Management Program.
fictionalized data	Fictional examples of similar situations that contain neither the identity of the taxpayer nor any information that could be considered attributable to a particular taxpayer. Such examples would not require any designation as sensitive.
FIPS	Federal Information Processing Standards.
FISMA	Federal Information Security Modernization Act of 2014.

Exhibit 10.5.1-1 (Cont. 2) (09-15-2023)

Glossary and Acronyms

Term	Definition or description
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. However, 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]
high security items	<p>High security items are original or certified paper documents containing SBU data (including PII and tax information), typically received and processed in IRS office critical or limited areas, that management must not allow to be removed from the facility.</p> <p>Note: These are “highly sensitive documents” in IRM 6.800.2 Employee Benefits, IRS Telework Program. Refer to IRM 10.2.14, the Protected Items / Information section.</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, see 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. 3) (09-15-2023)**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 Identity and Records Protection (IRP).
IRC	Internal Revenue Code.
IRP	Identity and Records Protection, under PGLD.
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 sub-categories:</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/Trap & Trace Reward Sex Crime Victim Terrorist Screening Whistleblower Identity <p>Some of the types of law enforcement data that the IRS might see includes grand jury, informant, and undercover operations information, and procedural guidance.</p>

Exhibit 10.5.1-1 (Cont. 4) (09-15-2023)
Glossary and Acronyms

Term	Definition or description
layered security	Where layered and complementary privacy and security controls are deemed sufficient to deter and detect unauthorized entry within the area. Examples include, but are not limited to, 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).
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/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 see include draft, pre-decisional, and deliberative information.</p>
limited area	Refer to IRM 10.2.14, the Limited Area section.
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 for testing, development, etc., in which case, it is no longer live. Live data often includes SBU data.</p>
MCD	Major Change Determination.
MER	Milestone Exit Release.
NDA	Non-Disclosure Agreement.
NIST	National Institute of Standards & Technology.
OFDP	Online Fraud Detection and Prevention, within IT Cybersecurity.
OneSDLC	<p>One Solution Delivery Life Cycle; replacing 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>

Exhibit 10.5.1-1 (Cont. 5) (09-15-2023)

Glossary and Acronyms

Term	Definition or description
other protected information	<p>Other protected information includes any knowledge or facts received by or created by IRS in support of IRS work. This includes all information covered by the Trade Secrets Act, the Procurement Integrity Act, and similar statutes. Examples include, but are not limited to:</p> <ul style="list-style-type: none"> • Records about individuals requiring protection under the Privacy Act. • Information that is not releasable under the Freedom of Information Act. • Proprietary data or proprietary business information. • Procurement sensitive data, such as contract proposals. • Information, which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government. • System sensitive information or Information Systems Vulnerability Information: <ul style="list-style-type: none"> a. Information related to the design and development of application source code. b. Specific IT configurations, where the information system security configurations could identify the state of security of that information system; Internet Protocol (IP) addresses that allow the workstations and servers to be potentially targeted and exploited; and source code that reveals IRS processes that could be exploited to harm IRS programs, employees, or taxpayers. c. Security information containing details of serious weaknesses and vulnerabilities associated with specific information systems and/or facilities. • Any information, which if improperly used or disclosed could adversely affect the ability of the IRS to accomplish its mission.
PCA	Privacy Compliance and Assurance.
PCLIA	Privacy and Civil Liberties Impact Assessment; replaced PIA for most privacy assessments. Refer to IRM 10.5.2 for more information.
personnel	<p>IRS personnel or users, which includes:</p> <ol style="list-style-type: none"> 1. Employees 2. Seasonal/temporary employees 3. Interns 4. Detailees 5. Consultants 6. IRS contractors (including contractors, subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers) <p>Subcategory of data in Privacy category.</p>

Exhibit 10.5.1-1 (Cont. 6) (09-15-2023)
Glossary and Acronyms

Term	Definition or description
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 there are many different types of information that can be used to distinguish or trace an individual’s identity, the term PII is necessarily broad. To determine whether information is PII, the agency must perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever more information becomes available – in any medium and from any source – that would make it possible to identify an individual.</p> <p>PII as defined here falls under the SBU data category called General Privacy, which is subcategory of the Privacy category. General Privacy refers to personal information, or, in some cases, “personally identifiable information,” as defined in OMB M-17-12, or “means of identification” as defined in 18 USC 1028(d)(7).</p>
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 for more information.
PIAMS	Privacy Impact Assessment Management System.
PII	Personally Identifiable Information.
POA&M	Plan of action and milestones.
PPC	Privacy Policy and Compliance.
PPKM	Privacy Policy and Knowledge Management, under PGLD’s Privacy Policy and Compliance (PPC).
privacy	Privacy at the IRS reflects the combined effort of the IRS, its personnel, and individual taxpayers to protect, control, and exercise rights over the collection, use, retention, dissemination, and disposal of personal information.
Privacy Compliance and Assurance (PCA)	Organization that owns and manages the PCLIA, BPRA, SBU Data Use programs for IRS.
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]

Exhibit 10.5.1-1 (Cont. 7) (09-15-2023)

Glossary and Acronyms

Term	Definition or description
privacy culture	Where all personnel think about privacy before acting. In such an environment or culture, protecting privacy guides the day-to-day practices and routines of everyone.
privacy and information lifecycle	<p>The series of uses and status of information. It includes the creation, collection, receipt, use, processing, maintenance, access, inspection, display, storage, disclosure, dissemination, or disposal of SBU data (including PII and tax information) regardless of format.</p> <p>Note: Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining. [NIST SP 800-53 PT-2]</p> <p>Information life cycle means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion. [OMB A-130]</p> <p>Also described as designation, safeguarding, marking, sharing (accessing and disseminating), destruction, and decontrol.</p>
Privacy Principles	The IRS Privacy Principles describe how the IRS protects an individual's right to privacy. Protecting taxpayer privacy and safeguarding confidential tax information is a public trust. To maintain this trust, the IRS and its personnel must follow the privacy principles.
privacy requirements	Mandatory IRS system requirements derived from IRS Privacy Principles and linked to the Privacy Controls, form the basis for privacy protection within the IRS. They mirror the IRS Privacy Principles and provide high-level privacy requirements applicable to the IRS Enterprise Architecture.
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 (see 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 Records and Information Management IRM 1.15 series for more information.

Exhibit 10.5.1-1 (Cont. 8) (09-15-2023)

Glossary and Acronyms

Term	Definition or description
requirements	<p>Per NIST SP 800-53, Section 2.1:</p> <p>For federal information security and privacy policies, the term <i>requirement</i> is generally used to refer to information security and privacy obligations imposed on organizations. For example, [OMB A-130] imposes information security and privacy requirements with which federal agencies must comply when managing information resources. The term <i>requirement</i> can also be used in a broader sense to refer to an expression of stakeholder protection needs for a particular system or organization. Stakeholder protection needs and the corresponding security and privacy requirements may be derived from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments).</p>
return	<p>Any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity (IRC 6103(b)(1)).</p> <p>Also falls under the SBU data subcategory called Federal Taxpayer Information, which is in the Tax category.</p>
return information	<p>In general, is any information collected or generated by the IRS with regard to any person's liability or possible liability under the IRC. IRC 6103(b)(2)(A) defines return information as very broad.</p> <p>Also falls under the SBU data subcategory called Federal Taxpayer Information, which is in the Tax category.</p>
RIM	Records and Information Management, under PGLD's Identity and Records Protection (IRP).
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 but is not necessarily limited to:</p> <ul style="list-style-type: none"> • Federal Tax Information (FTI), Personally Identifiable Information (PII), Protected Health Information (PHI), certain procurement information, system vulnerabilities, case selection methodologies, system information, enforcement procedures, investigation information. • Live data, which is production data in use. Live means that when changing the data, it changes in production. Authorized personnel may extract the data for testing, development, etc., in which case, it is no longer live. Live data often includes SBU data. <p>For more information about security protections of Sensitive But Unclassified (SBU) data, refer to IRM 10.8.1.</p>

Exhibit 10.5.1-1 (Cont. 9) (09-15-2023)

Glossary and Acronyms

Term	Definition or description
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 readability.
SLA	Staff-Like Access.
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, and/or process IRS information). • Possess physical and/or logical access to (including the opportunity to see, read, transcribe, and/or interpret) Sensitive but Unclassified (SBU) data, wherever the location. (See IRM 10.5.1 for examples of SBU data.) • Possess physical access to (including the opportunity to see, read, transcribe, and/or interpret) security items and products (e.g., items that must be stored in a locked container, security container, or a secure room, wherever the location. These items include, but are not limited to security devices/records, computer equipment, Identification media. Refer to IRM 10.2.14, the Protected Items / Information section. • Enter physical areas, wherever the location, that store/process SBU information (unescorted). <p>SLA is granted to an individual who is not an IRS employee (and includes, but is not limited to: contractors/subcontractors, whether procured by IRS or another entity, vendors, delivery persons, experts, consultants, paid/unpaid interns, other federal employees, cleaning/maintenance employees, etc.), and is approved upon required completion of a favorable suitability/fitness determination conducted by IRS Personnel Security.</p>
survey	Any data collection method, including but not limited to surveys, focus groups, interviews, pilot studies, and field tests. Refer to IRM 10.5.2 for more information.
synthetic data	Data that does not contain SBU data; however, 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. 10) (09-15-2023)
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	Information which is required to be published in the Federal Register by 5 USC 552a(e)(4). Refer to IRM 10.5.6, the Content of a System of Records Notice section.
tax information	<p>Any return or return information as defined in IRC 6103(b). This includes any information obtained, received, or generated by IRS or any Treasury component with respect to determining liability, potential liability, or amount of liability under the IRC.</p> <p>For this IRM, the terms <i>tax data</i> and <i>tax information</i> include <i>return</i> and <i>return information</i> as defined in IRC 6103(b).</p> <p>Tax information falls under the SBU data category called FTI or Tax. This IRM uses the term tax information to encompass all types of tax data. The Tax category includes:</p> <ul style="list-style-type: none"> • Federal 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 (1997) 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
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 (09-15-2023)**References**

This section lists the primary privacy statutes, regulations, guidelines, OMB Memoranda, and other materials that drive the privacy programs. You can find many of these on the Federal Privacy Council's website in the law library section.

<https://www.fpc.gov/law-library/>

Laws, Acts, Mandates, and OMB Memos

- Privacy Act of 1974 (5 USC 552a; Pub. L. No. 93-579), December 1974.
 - Computer Matching and Privacy Protection Act of 1988 (Pub. L. 100-503), which amended the Privacy Act of 1974 (1988).
 - Freedom of Information Act (FOIA) (1974).
- Note:** FOIA has been amended several times, the most significant of which for purposes of this IRM are: OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524 (2007); FOIA Improvement Act of 2016, Pub. L. 114-185.
- IRC 6103
 - E-Government Act (2002) [Pub.L. 107–347, 116 Stat. 2899, 44 USC 3501 Note, H.R. 2458/S. 803], December 2002.
 - Federal Information Security Modernization Act of 2014 (FISMA, Pub. L. No. 113-283, Title II), December 2014.
 - Protecting Americans from Tax Hikes Act of 2015
<https://www.congress.gov/bill/114th-congress/senate-bill/185/text>
 - Electronic Communications Privacy Act of 1986 (ECPA), 18 USC 2510 et seq.
 - Taxpayer First Act of 2019.

Executive Orders

The link for Executive Orders is:

<https://www.federalregister.gov/executive-orders>

- Executive Order 10450, Security Requirements for Government Employment, April 1953.
- Executive Order 13556, Controlled Unclassified Information, November 2010.
- Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013.
- Executive Order 13681, Improving the Security of Consumer Financial Transactions, October 2014.

OMB Circulars

<https://www.whitehouse.gov/omb/information-for-agencies/circulars/>

- OMB Circular No. A-11, Preparation, Submission, and Execution of the Budget
- OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
- OMB Circular No. A-130, Managing Information as a Strategic Resource

OMB Memos

<https://www.whitehouse.gov/omb/information-for-agencies/memoranda/>

The list of OMB Memos is:

- 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.

Exhibit 10.5.1-2 (Cont. 1) (09-15-2023)**References**

- 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-17-06 – Policies for Federal Agency Public Websites and Digital Services.
- 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-19-21 – Transition to Electronic Records.
- 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-23-03 – Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements.

Department of the Treasury

- Treasury Directive Publication (TD P) 15-71, Treasury Security Manual.
- *TD P 25-04 Privacy Act Handbook*.
- TD P 85-01, Treasury Information Technology (IT) Security Program, December 12, 2017.

IRS

On the IRS internal website::

- **Cybersecurity**
- **Authorized software**
- **Office of Disclosure** (*Disclosure)
- **Office of Safeguards** (*Safeguard Reports)
- **Privacy, Governmental Liaison and Disclosure** (email **Privacy*)
- **SA&A**
- Taxpayer Bill of Rights, codified in IRC 7803(a)(3):
<https://www.irs.gov/taxpayer-bill-of-rights>

Related IRMs:

- IRM 1.1.27, Organization and Staffing, Privacy, Governmental Liaison and Disclosure (PGLD)
- IRM 11.3 series, Disclosure of Official Information.
- IRM 1.15 series, Records and Information Management.
- IRM 10.8 series, especially:
 - IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance.
 - IRM 10.8.2, Information Technology (IT) Security, Roles and Responsibilities.
 - IRM 10.8.24, Information Technology (IT) Security, Cloud Computing Security Policy.
 - IRM 10.8.26, Information Technology (IT) Security, Government Furnished and Personally Owned Mobile Computing Device Security Policy.
 - IRM 10.8.27, Information Technology (IT) Security, Personal Use of Government Furnished Information Technology Equipment and Resources.

Exhibit 10.5.1-2 (Cont. 2) (09-15-2023)**References**

- IRM 10.10.3, Centralized Authentication Policy – Centralizing Identity Proofing for Authentication Across All IRS Channels.
- IRM 10.23.2, Personnel Security, Contractor Investigations.

NIST

The link for National Institute of Standards and Technology (NIST) Special Publication (SP) for the most recent versions:

<https://csrc.nist.gov/publications/sp>

- SP 800-18, Guide for Developing Security Plans for Federal Information Systems, February 2006.
- SP 800-28 Version 2, Guidelines on Active Content and Mobile Code, March 2008.
- SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012.
- SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018.
- SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011.
- SP 800-44 Version 2, Guidelines on Securing Public Web Servers, September 2007.
- SP 800-45 Version 2, Guidelines on Electronic Mail Security, February 2007.
- SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, July 2016.
- SP 800-47 Rev. 1, Managing the Security of Information Exchanges, July 2021.
- SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, December 2020.
- SP 800-59, Guideline for Identifying an Information System as a National Security System, August 2003.
- SP 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.
- SP 800-63, Digital Identity Guidelines, March 2020:
 - a. Digital Identity Guidelines: Enrollment and Identity Proofing.
 - b. Digital Identity Guidelines: Authentication and Lifecycle Management.
 - c. Digital Identity Guidelines: Federation and Assertions.
- SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, July 2013.
- SP 800-88 Rev. 1, Guidelines for Media Sanitization, December 2014.
- SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010.
- SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, September 2011.
- SP 800-163 Rev. 1, Vetting the Security of Mobile Applications, April 2019.
- SP 800-183, *Networks of 'Things'*, July 2016.

The link for FIPS publications is:

<https://csrc.nist.gov/publications/fips>

- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.
- Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
- Federal Information Processing Standards (FIPS) Publication 201-3, Personal Identity Verification of Federal Employees and Contractors.

Exhibit 10.5.1-2 (Cont. 3) (09-15-2023)

References

More information about the NIST publications noted above is available on the NIST website:

<https://csrc.nist.gov/>

IAPP

The link for International Association of Privacy Professionals (IAPP):

<https://www.iapp.org>

