PRIVACY, GOVERNMENTAL LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

Date of Issuance: 10-23-2024

Control Number: PGLD-10-1024-0021
Expiration Date: 10-23-2026
Affected IRM(s): 10.5.1

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

FROM: John E. Lyons */s/ John E. Lyons*
Director, Privacy Policy and Compliance

SUBJECT: Contract Privacy Requirements

This memorandum issues privacy policy interim guidance on contract privacy requirements and is effective as of October 23, 2024. Please distribute this information to all affected personnel within your organization, such as IRS contracting officers (COs), contracting officer's representatives (CORs), and other personnel engaged in contract-related activities.

Purpose: This interim guidance implements privacy policy to clarify contract privacy requirements and mandatory language, referencing previously existing contract requirements in the renamed IRM 10.5.1.4.7, Personnel in Contract Activities (formerly Personnel Engaged in Procurement Activities), and moving the details from that subsection to renamed IRM 10.5.1.6.15, Contracts (formerly Contractors), as new subsections. It also clarifies two security and privacy controls related to contracts.

Background/Source(s) of Authority: This interim guidance falls under the authorities listed in Privacy Policy IRM 10.5.1.1.6, Authority.

Procedural Change: The procedural changes in the attached interim guidance apply.

Effect on Other Documents: We will incorporate this interim guidance into IRM 10.5.1, by October 23, 2026.

Effective Date: October 23, 2024

Contact: If you have any questions, please email the Associate Director, Privacy Policy, at *Privacy.

Distribution: FOIA Library (external) on IRS.gov.

Attachment Interim Guidance: PGLD-10-1024-0021

Interim Guidance: PGLD-10-1024-0021

The following changes take effect October 23, 2024**, for** IRM 10.5.1.

10.5.1.4.7
(10-23-2024)
Personnel ~~Engaged~~ in ~~Procurement~~ Contract Activities

(1) In addition to the Employee and Personnel responsibilities, IRS contracting officers (COs), contracting officer's representatives (CORs), and other personnel engaged in ~~procurement~~ contract-related activities ~~involving SBU data (including PII and tax information) must address these items~~ must follow the requirements in these subsections, if they apply to their respective roles [Privacy Act, IRC 6103(n), OMB A-130]:

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

a. IRM 10.5.1.6.15, Contracts
b. IRM 10.5.1.6.15.1, Contract Privacy Requirements Language
c. IRM 10.5.1.6.15.2, Contracting Officer Representative (COR) Training
d. IRM 10.5.1.6.15.3, OneSDLC in Contracts
e. IRM 10.5.1.6.15.4, Privacy Act in Contracts
f. IRM 10.5.1.6.15.5, IRC 6103 (Tax Information) in Contracts
g. IRM 10.5.1.6.15.6, Background Investigation
h. IRM 10.5.1.6.15.7, Mandatory Training for Contractors
i. IRM 10.5.1.6.15.8, Non-Disclosure Agreements
j. IRM 10.5.1.6.15.9, Privacy and Security Controls in Contracts
k. IRM 10.5.1.6.15.10, Privacy and Civil Liberties Impact Assessment (PCLIA) in Contracts
l. IRM 10.5.1.6.15.11, Testing and Development Environments in Contracts
m. IRM 10.5.1.6.15.12, Incident Response in Contracts
n. IRM 10.5.1.6.15.13, Unauthorized Access (UNAX) in Contracts
o. IRM 10.5.1.6.15.14, Contract Closeout
p. IRM 10.5.1.6.15.15, Federal Acquisition Regulation (FAR) Compliance
q. IRM 10.5.1.8.10.13, PM-17 Program Management -- Protecting Controlled Unclassified Information on External Systems [J] {Org}
r. IRM 10.5.1.8.14.3, SA-04 System and Services Acquisition – Acquisition Process [J] {Sys}

~~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, protections, 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 PCLIAs 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

(2) In this IRM, contract privacy requirements apply to contractors, subcontractors, contractor employees, and subcontractor employees. Contract requirements flow down to subcontracts (which the IRS must approve) under the internal IRS Acquisition Policy (IRSAP) site Index C (pdf).

(3) For more procurement information, refer to the internal Office of the Chief Procurement Officer Customer Portal.

(4) For more privacy information, refer to the internal Contractor Compliance site.

(5) Email privacy policy for help with these responsibilities at *Privacy.

10.5.1.6.15
(10-23-2024)
Contracts ~~Contractors~~

(1) The IRS defines ~~as~~ personnel ~~as~~ to include contractors in IRM 10.5.1.1.2, Audience. ~~so they~~ Contractors and applicable IRS personnel must follow the requirements in IRM 10.5.1.4.1, Employees/Personnel.

(2) The IRS has statutory and regulatory privacy obligations for contracts ~~contractors with access to SBU data (including PII and tax information)~~. To meet these obligations, the Chief Privacy Officer (CPO) as designee of the Senior Agency Official for Privacy (SAOP), must make sure the IRS: ~~As outlined in the IRS Privacy Principle of Accountability, and NIST Privacy Controls, the IRS must~~ [Privacy Act, IRC 6103(n), OMB A-130, NIST, Accountability]

a. Establishes privacy roles, responsibilities, oversight, and access requirements for contractors and service providers throughout the privacy lifecycle. ~~[OMB A-130]~~
b. Includes privacy requirements for all relevant stages of the privacy lifecycle in contracts and other acquisition contract-related documents, including end of contract.
c. Follows Privacy Act and IRC requirements for contracts ~~contractors~~, outlined in IRM 10.5.6.2.9.1, ~~the~~ Privacy Act Contract Requirements, ~~section~~ and IRM 11.3.24.2, Requirements.

(3) The IRS CO, COR, and others responsible for contract-related activities ~~on contracts that involve SBU data (including PII and tax information) must meet~~ must follow the requirements in these subsections, if they apply to their respective roles: ~~IRM 10.5.1.4.7, Personnel Engaged in Procurement Activities.~~

a. IRM 10.5.1.4.7, Personnel in Contract Activities
b. IRM 10.5.1.6.15.1, Contract Privacy Requirements Language
c. IRM 10.5.1.6.15.2, Contracting Officer Representative (COR) Training
d. IRM 10.5.1.6.15.3, OneSDLC in Contracts
e. IRM 10.5.1.6.15.4, Privacy Act in Contracts
f. IRM 10.5.1.6.15.5, IRC 6103 (Tax Information) in Contracts
g. IRM 10.5.1.6.15.6, Background Investigation
h. IRM 10.5.1.6.15.7, Mandatory Training for Contractors
i. IRM 10.5.1.6.15.8, Non-Disclosure Agreements
j. IRM 10.5.1.6.15.9, Privacy and Security Controls in Contracts
k. IRM 10.5.1.6.15.10, Privacy and Civil Liberties Impact Assessment (PCLIA) in Contracts
l. IRM 10.5.1.6.15.11, Testing and Development Environments in Contracts
m. IRM 10.5.1.6.15.12, Incident Response in Contracts
n. IRM 10.5.1.6.15.13, Unauthorized Access (UNAX) in Contracts
o. IRM 10.5.1.6.15.14, Contract Closeout
p. IRM 10.5.1.6.15.15, Federal Acquisition Regulation (FAR) Compliance
q. IRM 10.5.1.8.10.13, PM-17 Program Management -- Protecting Controlled Unclassified Information on External Systems [J] {Org}
r. IRM 10.5.1.8.14.3, SA-04 System and Services Acquisition – Acquisition Process [J] {Sys}

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

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

(5) For more procurement information, refer to the internal Office of the Chief Procurement Officer Customer Portal.

(6) For more privacy information, refer to the internal Contractor Compliance site.

(7) Email privacy policy for help with these responsibilities at *Privacy.

10.5.1.6.15.1
(10-23-2024)
Contract Privacy Requirements Language

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

(2) The IRSAP requirements provide binding internal policy to the IRS for all IRS acquisitions. The requirements language in a contract legally binds the contractor. Per the IRSAP, the Office of the Chief Procurement Officer (OCPO) must use the IRSAP to ensure adherence to IRS-specific policy. The IRS must use the IRSAP in conjunction with the DTAP, DTAR, and FAR to ensure adherence to all Treasury and IRS policies and federal procurement regulations.

(3) In addition to the SBU data contract requirements language, include in the solicitation, request for proposal, contract, statement of work (or similar document, such as task order, performance work statement, or statement of objectives), and work order [Privacy Act, IRC 6103(n)]:
   a. Business need and justification for how the contractor will use the data.
   b. Specific data elements.
   c. Authorized purpose and use (legal authority that allows us to share the data).
   d. Who will receive the data.
   e. How to protect the data at rest and in transit.
   f. What happens to the data after the need ends.

   Note: Review IRM 10.5.1.6.15.4, Privacy Act in Contracts, and IRM 10.5.1.6.15.5, IRC 6103 (Tax Information) in Contracts.

(4) For an exception to the requirement to include the privacy requirements language in a contract, you must get approval from privacy. Email your exception request (with documentation) to the *Privacy mailbox for approval. Include Privacy's approval response in your procurement shopping cart.

10.5.1.6.15.2
(10-23-2024)
Contracting Officer Representative (COR) Training

(1) Review and understand the proper privacy contract-related training and guidance, including the COR Security, Privacy, and Disclosure Awareness Training.
(2) For more information, refer to the internal COR Community of Practice (CCOP) site.

10.5.1.6.15.3
(10-23-2024)
OneSDLC in Contracts

(1) Follow the One Solution Delivery Life Cycle (OneSDLC) process.
(2) For more information about OneSDLC, refer to IRM 2.31.1, One Solution Delivery Life Cycle Guidance, or the internal OneSDLC site.

10.5.1.6.15.4
(10-23-2024)
Privacy Act in Contracts

(1) Contract work statements (or similar documents) must specifically name the proper System of Records Notice (SORN) when Privacy Act information is a part of the research, design, development, testing, or operation work under the contract.
(2) Include the Privacy Act authority, use, protections, and penalties for violations.
(3) For more information, review IRM 10.5.1.6.15.1, Privacy Contract Requirements Language, and refer to IRM 10.5.6.2.9.1, Privacy Act Contract Requirements.

10.5.1.6.15.5
(10-23-2024)
IRC 6103 (Tax Information) in Contracts

(1) When the contract involves tax information, the contract must include IRC 6103 authority, use, protections, prohibitions on redisclosure (secondary use of data), and penalties for violations. [IRC 6103(n)]
(2) For more information, review IRM 10.5.1.6.15.1, Privacy Contract Requirements Language, and refer to IRM 10.5.6.2.9.1, Privacy Act Contract Requirements, and IRM 11.3.24.2, Requirements.

10.5.1.6.15.6
(10-23-2024)
Background Investigation

(1) Support the proper level of contractor background investigation in cooperation with the Office of Personnel Security (PS), Contract Security Onboarding (CSO), per IRM 10.23.2.2.1, Vendor and Contracting Officer's Representative Roles.
(2) This includes working with PS to assign the correct risk designations (often Moderate for access to SBU data), helping coordinate contractor fingerprinting, and distributing identity cards, if needed.
(3) For position risk designations, following IRM 10.23.2, Contractor Investigations:
    a. All contracting actions with SBU data (including PII and tax information), with few exceptions, carry a moderate impact security level as public trust positions.
    b. Public Trust positions involve access to, operation, or control of proprietary systems of information, such as financial or personal records, with a

significant risk for causing damage to people, programs, or an agency, or for realizing personal gain [OPM suitability guidance]. Per Treasury policy, public trust positions are moderate and high risk [TD P 15-71]. Per IRM 10.23.3.6, Investigative Tiers, the minimum investigative requirements for IRS public trust positions as recommended by the Department of the Treasury and OPM are:

- Tier 2 – Moderate Risk
- Tier 4 – High Risk

c. When assigning a risk designation, you must consider the level of IRS supervision over the individual with access to SBU data. For contractors (especially off-site), their ability to act independently with only occasional review by the IRS limits the level of IRS supervision.
d. Contracts with staff-like access to FISMA systems carry a High impact security level.

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

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

10.5.1.6.15.7
(10-23-2024)
Mandatory Training for Contractors

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

10.5.1.6.15.8
(10-23-2024)
Non-Disclosure Agreements

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

10.5.1.6.15.9
(10-23-2024)
Privacy and Security Controls in Contracts

(1) Contracts must reference and contractors must follow Pub 4812, Contractor Security & Privacy Controls.
(2) Pub 4812 incorporates requirements from IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls, and the relevant 10.8 series IRMs.

10.5.1.6.15.10
(10-23-2024)
Privacy and Civil Liberties Impact Assessment (PCLIA) in Contracts

(1) Contractors must receive and understand the PCLIA when supporting a project with a PCLIA. [RA-08]
Note: The IRS requires PCLIAs for systems, pilot projects, research, experimentation, the use of innovative technologies, technical demonstrations, prototypes, and proof of concepts, surveys, and the like.
(2) In some cases, contractors might need to work with the IRS to complete the required PCLIA.
(3) Before developing or procuring information technology that uses PII, the IRS must complete a PCLIA. [E-Government Act]
(4) For more information about the PCLIA process, refer to IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA) and the internal PCLIA site.

10.5.1.6.15.11
(10-23-2024)
Testing and Development Environments in Contracts

(1) Contracts involving the use of SBU data in testing and development environments must follow the requirements of IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments.
(2) For more information, refer to the internal SBU Data Use Process site.

10.5.1.6.15.12
(10-23-2024)
Incident Response in Contracts

(1) Make sure the contractor understands incident response and their timely reporting requirements.
(2) Immediately report all incidents related to IRS processing, information, or information systems upon discovery to the CO and COR.
(3) Report security incidents to the Computer Security Incident Response Center (CSIRC) by contacting the CSIRC Support Desk at 240-613-3606.
(4) Refer to Pub 4812, the IR-6 Incident Reporting section.

10.5.1.6.15.13
(10-23-2024)
Unauthorized Access (UNAX) in Contracts

(1) Report unauthorized access (UNAX) by a contractor to TIGTA, the CO, and COR.
(2) For more information on UNAX, review IRM 10.5.1.2.5, UNAX, and refer to IRM 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements, and the internal UNAX site.

10.5.1.6.15.14
(10-23-2024)
Contract Closeout

(1) Begin the closeout process in time to complete closeout before the contract ends to maintain proper protection and control of SBU data.
(2) Collaborate with Contractor Security Management (CSM) at contract closeout to revoke system and facilities access.
(3) Contractors and those responsible must return all IRS data or dispose of it as required by the contract.
(4) Refer to the IRM 1.15 series, Records and Information Management to comply with paper and electronic records management requirements.

10.5.1.6.15.15
(10-23-2024)
Federal Acquisition Regulation (FAR) Compliance

(1) Follow the Federal Acquisition Regulations (FAR) for all contracts.
(2) For more information, refer to the FAR (external) site.

10.5.1.8.10.13
(10-DD-2024)
PM-17 Program Management -- Protecting Controlled Unclassified Information on External Systems [J] {Org}

(1) This is a joint security and privacy control about protecting controlled unclassified information (CUI) on external systems. For the full text of the control, refer to IRM 10.8.1.4.13.17, PM-17 Protecting Controlled Unclassified Information on External Systems.
(2) ~~The privacy concerns are that~~ The IRS requires that our partners protect all sensitive information ~~is protected~~ on external systems by following the privacy policy in IRM 10.5.1.6.15, Contracts. This means including all privacy requirements language in all contracts, with few approved exceptions.
(3) **Implementation guidance:** The IRS uses SBU data to describe what this control calls CUI. The IRS implements this control by requiring ~~that~~ contractors and external partners to protect all SBU data (including PII and tax information)~~, which~~ This means all IRS acquisitions and agreements ~~contain proper~~ must include required language holding contractors, subcontractors, and other service providers accountable for following federal and IRS privacy policies and procedures.~~, such as~~ Examples of such policies include privacy ~~clauses~~ requirements language in contracts, PCLIAs for contracted IT, security and privacy controls, and defining contractors as IRS personnel in this IRM with all the same responsibilities for data protection.

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

(4) To meet this control, you must follow the policies in this IRM ~~throughout, and specifically, PGLD policies~~ on the protecting controlled unclassified information (SBU data) on external systems control, including ~~include, but are not limited to, the sections~~:

a. IRM 10.5.1.4, IRS-Wide Privacy Roles and Responsibilities (Personnel ~~Engaged~~ in Procurement ~~Co~~ntract Activities)
b. IRM 10.5.1.6.15, Contract~~or~~s
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

Note: Where this policy cites a subsection, it includes by reference its subsections. For example, the reference to subsection IRM 10.5.1.6.15, Contractors, also includes its 15 subsections, from IRM 10.5.1.6.15.1, Contract Privacy Requirements Language, to IRM 10.5.1.6.15.15, Federal Acquisition Regulation (FAR) Compliance.

(5) Follow the other PGLD and IRS policies also that address the protecting controlled unclassified information (SBU data) on ~~extern~~al systems control, including in the following:

~~a.~~ ~~IRM~~ 10.5.2.2.4, System PCLIAs
b. IRM 10.5.2.2.5.1, Survey PCLIA
c. IRM 10.5.2.2.5.2, Shared Storage PIAs
d. IRM 10.5.4.3, Reporting Losses, Thefts, and Disclosures
e. IRM 10.5.5.3.4, Contracting Officer's Representative (COR) UNAX Responsibilities
f. IRM 10.5.5.3.5, Employee UNAX Responsibilities
g. IRM 10.5.6.1.3, Roles and Responsibilities
h. IRM 10.5.6.2.8, Privacy Act Training
i. IRM 10.5.6.2.9.1, Privacy Act Contract Requirements
j. IRM 11.3.24.2, : throughout, and specifically Requirements
k. IRM 11.3.36.2, ~~: throughout, and specifically~~ Legal Requirements
l. IRM 11.4.1.13, ~~: throughout, and specifically~~ Data Exchange Agreements Governmental ~~Liaisons~~ ~~Procedures for Routing, Approving, Signing and Terminating Basic Agree~~ements (BAs), Implementing Agreements (IAs), Memorandums of Understanding (MOUs), and Other Agreements
m. IRM 1.15.1.1.3, Responsibilities
n. Document 13347 (pdf), Data Breach Response Playbook: Section 5.4, External Third-Party Incidents
o. Document 13347-A, IRS Data Breach Response Plan: Section 2.5, Contractors

10.5.1.8.14.3
(10-DD-2024)
SA-04 System and Services Acquisition -- Acquisition Process [J] {Sys}

(1) This is a joint security and privacy control about the acquisition process. For the full text of the control, refer to IRM 10.8.1.4.17.3, SA-04 Acquisition Process.

(2) The IRS requires ~~privacy concerns are that~~ including privacy protections in contracts ~~provisions incorporate privacy protections~~ by following IRM 10.5.1.6.15, Contracts. This means including all privacy requirements language in all contracts, with few approved exceptions.

(3) Implementation guidance: The IRS implements this control by requiring all IRS acquisitions and contract vehicles ~~contain proper~~ include required language holding contractors and other service providers accountable for following federal and IRS privacy policies and procedures, such as privacy requirements language ~~clauses~~ in contracts, PCLIAs for contracted IT solutions, security and privacy controls, and defining contractors as IRS personnel in this IRM with all the same responsibilities for data protection.

(4) To meet this control, you must follow the policies ~~in this IRM, PGLD policies~~ on the acquisition process control, ~~include, but are not limited to, the sections~~ listed in the SA-01 references, IRM 10.5.1.8.14.