Date of Approval: 05/28/2026
Questionnaire Number: 2874

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Scanned Paper Returns (SPR), Zero Paper Initiative (ZPI) - Iron Mountain

Acronym:

SPR ZPI - Iron Mountain

Business Unit

Taxpayer Services

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

Taxpayer Services utilizes the Digitalization-as-a-Service (DaaS) contract for Scanned Paper Return (SPR) and other paper received at the IRS to multiple internal system(s) as a document intake solution that will increase data collection up front, optimize electronic file storage, and achieve full data capture for paper submissions. This is needed to increase digital intake for the Zero Paper Initiative (ZPI). The system is used by external vendors to transmit digital data from paper tax returns via the Modernized e-File (MeF) system and Kiteworks. Tax return information is scanned using Optical Character Recognition (OCR) at external vendors sites and transmitted to the IRS via MeF and Kiteworks. IRS employees access the data stored in Modernized Tax Return Database (MTRDB) via Employee User Portal (EUP), Digital Content Retrieval (DCR), and other downstream Systems. Full data capture for paper Information Returns and

Correspondence submitted by taxpayers will soon follow. Thus, the SPR platform is effectively utilized in achieving the goal of reducing paper volume, increasing access to digital data, and preparing the IRS to manage the digital data.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

This project contains Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), and Federal Tax Information (FTI) from taxpayer submissions. This sensitive taxpayer information is required for each tax return. The information that is received from other internal IRS systems is used to validate sensitive data. The Transmitter and Electronic Return Originator (ERO) information received from the transmitter is matched against the data collected from internal IRS systems. After the paper forms are scanned in through the external contractors, they are prepared as electronic returns and go through document perfection to be transitioned to the Modernized e-file (MeF) or Digital Content Retrieval (DCR) compliant format so that they can be electronically submitted to the IRS. Each paper document prepared and submitted to IRS systems must adhere to the schemas and business rules. If a single data element fails the schema integrity check or has a business rule failure, the document is rejected. Electronic Tax Administration (ETA) supplies the business rules for each return type. MeF enforces rules against the tax returns using a business rules engine. Business rules enforce relationships between data and forms. When MeF validates returns against the business rules, if it encounters a discrepancy, the tax return is rejected. New schemas and business rules are issued for each new tax year. Any non-current returns (prior tax years) prepared and submitted must use that year's schema and business rule versions or the returns will fail the schema and business rule validation checks. Only validated submissions that pass the schema and business rule validation checks are accepted as electronic submissions into IRS systems allowing for subsequent destruction of the corresponding paper submission.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address
Agency Sensitive Information
Employer Identification Number
Employment Information

Name
Protected Information
Social Security Number (including masked or last four digits)
Tax ID Number
Telephone Numbers

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this a new system?
No

1.1 Is there an approved Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?
Yes

1.11 Has the name changed since the prior PCLIA?
No

1.13 What is the Acronym on the most recent approved PCLIA?
SPR (Scanned Paper Returns)

1.2 What changes occurred to require this updated PCLIA?
This is being broken out into multiple PCLIAs due to multiple vendors and changes to Publication 4812.

2 What is the name of the contractor?
Iron Mountain

3 Please provide a contact person for the contractor.
XXX XX

4 Please provide the phone number for the contractor.
XX XXXX

5 What is the email address for the contractor?
XXX XXX

6 What is the address for the contractor?
[XXXX XXXXX X]

7 What is the location of the contractor?
[XXX XXX]

8 What is the contract number?
GS03F049GA

9 What is the length of the contract?
One (1) year plus four (4) option years

10 What is the contract start date?
September 15, 2025

11 What is the contract end date?
September 14, 2026

12 What is the Contracting Officer (CO) name?
[XX XX]

13 What is the CO's email address?
[XX XXXX X]

14 What is the CO's phone number?
XX XX X

15 Who is the Contracting Officer's Representative (COR)?
[XX XX X]

16 What is the COR's email address?
[XX X]

17 What is the COR's phone number?
[XX XXX]

18 What is the IRS business unit procuring the contract?
Information Technology

19 What is the business owner contact name?
XX XX

20 How is access to the SBU/PII determined and by whom?
Internal Users (IRS Employees): Internal Users are subject to management, system administrator, data administrator, and security administrator approval via the Business Entitlement Access Request Service (BEARS). BEARS is used to document access requests, modifications, terminations for all types of users,

including system administrators, system accounts requiring Electronic File Transfer Utility (EFTU) access, and test accounts. Contractors: Users request access to the Integrated Enterprise Portal (IEP) environment through the Information Technology Security Management (ITSM) authorization process. To request a new account, changes to an existing account or removal of an account, the IRS Enterprise Portals Contractor Access Form is filled out. Upon completion of the form, the Program Management Office (PMO) resource will validate the request and create an access grant request within ITSM. ITSM will route the ticket to the appropriate task-order lead to review and approve the requested level of access. Once approval is received, the ticket will be routed to the appropriate task order staff to create, edit, disable or remove the account. Access will be approved in accordance with the principle of least privilege based on the intended system usage of the user. Administrators will only grant access permissions commensurate with the level authorized in the ITSM ticket. Other External Users: Other external users apply for Staff-Like Access (SLA) through e-Services. They must pass a suitability background investigation before being given access rights. When they pass the suitability background process, they are provided their Electronic Transmitter Identifying Number (ETIN) and Electronic Filer Identifying Number (EFIN). This process is external to MeF. For external third party and State Trading Partners who access Application to Application (A2A) or Internet Filing Application (IFA) through the Registered User Portal (RUP), account registration is performed through e-services and stored within Enterprise Directory and Authentication Services (EDAS). The application process mentioned above determines user's Role Based Access to MeF. External trading partners are required to use certificate-based authentication. A2A users must enroll their systems using the E-Services Automated Enrollment application. The application uses the user's e-services profile to determine access rights. Transmitters are given transmitter access and roles but denied State agency roles. State agencies are given State agency access and roles but denied transmitter roles. A definition with a detailed description of SLA is outlined in Publication 4812.

21 Are any authorized employees approved for telework?

Yes

21.1 Is there an approved telework agreement/policy?

Yes

22 Describe the work to be performed, how PII will be used, collected, received, displayed, stored, maintained, or disseminated.

The DaaS Contractors perform controlled intake, scanning, data extraction, validation, transmission, and destruction of IRS paper submissions related to tax returns, information returns, and correspondence, some of which contain PII and FTI. All PII handling is strictly limited to IRS mission purposes and governed by Publication 4812, IRS IRMs, NIST standards, FedRAMP requirements, and federal privacy law. Iron Mountain uses Google Document AI software to

perform Optical Character Recognition (OCR) on scanned documents. They use Iron Mountain InSight as their Cloud Service Provider (CSP), which has a FedRAMP ID R2031155471 and a Moderate authorized status currently (the platform received an IRS Authority to Operate (ATO) on 1/20/2026 and the FedRAMP PMO is currently reviewing the FedRAMP High package) FedRAMP High authorized status as they currently are listed in agency-review status). Iron Mountain does not employ offshore support for this project and there is no offshore support for CSP.

A. Description of Work to be Performed - Under the ZPI DaaS contract, the Contractor performs centralized intake, scanning, digitalization, data extraction, transmission, and controlled destruction of paper submissions of tax returns, information returns, and correspondence from taxpayers received by the IRS.

I. Document Receiving

• Physically receiving inbound IRS mail (tax returns, amended returns, information returns, and correspondence)
• Logging and barcoding submissions upon receipt
• Digitally stamping received date
• Reconciling receipt volumes with USPS and IRS tracking systems
• Maintaining chain-of-custody controls

II. Sorting and Classification

• Sorting by form type and submission category
• Identifying unprocessable or out-of-scope documents
• Separating remittances from forms
• Securing and expediting discovered remittances (cash, etc.)
• Shipping non-check remittances using secure procedures
• Forwarding unprocessable or legally sensitive materials to IRS within one week required timeframes

III. Digitalization & Data Extraction

• High-resolution scanning of documents (front/back of envelope included)
• Optical Character Recognition (OCR) / Intelligent Character Recognition (ICR)
• Data extraction into structured formats (XML, JSON, PDF metadata)
• Indexing per IRS schema and System Requirements for Industry Partners (SRIP)
• Transmitting digitized data via secure electronic file transfer to IRS ingestion systems (MeF, IRIS, AIR, GMF, FATCA, CSS)

IV. Quality Assurance & Validation

• Conducting Quality Assurance Reviews (QAR)
• Performing 10% sampling per IRS RIM guidelines
• Comparing paper source documents to XML metadata
• Ensuring ≥ 85% field accuracy and ≥ 95% OCR threshold
• Preventing destruction until IRS validation complete

V. Secure Retention & Destruction

• Retaining paper for up to 60 days post-validation

• Destroying paper per NIST SP 800-88 standards
• Providing destruction confirmation documentation

B. How PII Is Used - PII is not used for marketing, profiling, analytics beyond IRS mission requirements, or any non-contractual purpose. PII is used strictly for the following:
• Converting paper submissions into machine-readable digital records
• Supporting ingestion into IRS systems (MeF, IRIS, AIR, GMF, FATCA, CSS)
• Validating data accuracy against source documents
• Processing remittances
• Supporting compliance and audit requirements
• Fulfilling IRS operational requirements

C. How PII Is Collected - PII is collected by the following:
• Receiving paper submissions directly from taxpayers via USPS or authorized forwarding
• Receiving remittances and attachments included in tax return packages
• Scanning physical documents into digital image format
• Extracting structured data fields using OCR/ICR technologies
• The Contractor does not independently solicit or create PII; PII originates from taxpayer submissions

D. How PII Is Received - PII is received through the following:
• Physical mail shipments to Contractor facilities
• Secure shipping containers and chain-of-custody processes
• Barcoded intake tracking
• Secure digital transmission between Contractor and IRS systems (EFT, metadata transfer)

E. How PII Is Displayed - PII may be displayed through the following:
• On scanned images within Contractor secure systems
• During Quality Assurance Review comparisons (paper vs XML)
• Within secure dashboards accessible only to authorized personnel
• On audit logs and transmission confirmations
• Access is strictly role-based and limited to authorized personnel with Staff-Like Access approval

F. How PII Is Stored - PII is stored as follows:
• Temporarily in Contractors' secure facilities
• Within encrypted digital systems
• In compliance with IRS Publication 4812
• In accordance with NARA guidelines, IRS IRM 10.5.1 (Privacy), and NIST SP 800-88 (Media Sanitization)
• Within FedRAMP High-compliant cloud environments (by January 1, 2026, requirement)
• In secure containers for physical discovered remittances

• For up to 60 days post-validation prior to destruction

G. How PII Is Maintained - Maintenance includes the following:
• Maintaining audit logs (who accessed, when, what was modified)
• Monitoring quality control checkpoints
• Conducting background investigations for all personnel
• Annual UNAX and Security Awareness Training
• Following strict incident reporting procedures (OMB 17-12)
• Maintaining encryption and firewall controls
• Controlling physical access to facilities and systems

H. How PII Is Disseminated - PII is never sold, shared externally, disclosed without authorization, or used outside IRS' mission scope. PII is disseminated only:
• Back to IRS systems through secure electronic file transmission
• To IRS Submission Processing Campuses for unprocessable materials
• To authorized IRS personnel for validation and ingestion

23 Provide a clear, concise reason why the contractor will use the PII, the benefit to IRS, and how the information will be used.

A. Purpose for Contractor Use of PII - The contractor uses PII solely to convert paper taxpayer submissions into accurate, machine-readable digital records for processing within IRS systems. The contractor does not independently collect, analyze, or use PII for any purpose outside of fulfilling IRS-directed digitization and transmission requirements.

B. Benefit to the IRS – Vendors' work under the DaaS contract supports the IRS mission by modernizing submission processing and improving taxpayer service outcomes. The contractors' use of PII enables:
• Faster intake and processing of tax returns and correspondence
• Reduced manual data entry and transcription errors
• Improved cycle times and operational efficiency
• Enhanced tracking, auditability, and accountability
• Lower paper handling and storage costs • Greater surge capacity during peak filing periods

C. How the Information Will Be Used - PII will only be accessed by authorized personnel with appropriate background investigations and training, and only for the purpose of performing contractually required digitization activities. The contractors will use PII to:
• Scan and create digital images of submitted documents
• Extract structured data (e.g., SSNs, income amounts, tax year) into IRS-approved formats (XML, JSON, PDF metadata)
• Validate extracted data against source documents through quality review
• Transmit digitized data securely to IRS ingestion systems (e.g., MeF, IRIS)
• Facilitate remittance processing within required timeframes

• Retain paper temporarily for validation and securely destroy it in accordance with IRS and NIST standards

24 Please indicate the location where the work will be performed, and how the data will be processed, stored, and secured.

A. Location(s) Where Work Will Be Performed - [XXXX X]

B. How the Data Is Processed - Data will be processed through a secure, IRS-approved digitization workflow in which paper submissions are barcoded and logged upon arrival at the contractors' secure facility, scanned producing high-resolution images (including front/back of envelopes), data is extracted using OCR technology that extracts structured data into IRS-approved formats (e.g., XML, JSON, PDF metadata), validated for accuracy through Quality Assurance Reviews that compare digital output to the original paper submission, and the digitized files are securely transmitted to IRS systems (e.g., MeF, IRIS, GMF, etc.) via encrypted electronic file transfer.

C. How the Data Is Stored - The information will be temporarily stored in encrypted, access-controlled environments that meet IRS Publication 4812 and FedRAMP High security requirements. While being stored for up to 60 days following IRS validation, all paper remains secured in locked containers compliant with IRA and NARA standards.

D. How the Data Is Secured - Strict administrative, technical, and physical safeguards, including background investigations, role-based access controls, audit logging, encryption, and NIST-compliant destruction procedures, are used to protect PII and Federal Tax Information throughout its lifecycle. In addition, the contractors do not independently analyze or retain the data beyond what is required to fulfill IRS-directed processing and validation.

Administrative Controls
• Moderate background investigations for all personnel
• Staff-Like Access approval by IRS Personnel Security
• Annual Security Awareness Training (SAT) and UNAX certification
• Written Quality Control and Incident Response procedures
• Compliance with IRS Publication 4812 and IRM 10.5.1

Technical Controls
• Encryption of data in transit and at rest
• FedRAMP High cloud security standards (by Jan 1, 2026)
• Firewall, intrusion detection, and access logging
• Multi-factor authentication where applicable
• Secure file transfer protocols
• Daily audit log retention in IRS-approved formats

Physical Controls
• NARA-compliant facilities

• Access-controlled workspaces
• Double packaging and labeling of shipments
• Secure remittance containers
• NIST SP 800-88 compliant shredding for destruction

B. How the Data Is Processed - Data will be processed through a secure, IRS-approved digitization workflow in which paper submissions are barcoded and logged upon arrival at the contractors' secure facility, scanned producing high-resolution images (including front/back of envelopes), data is extracted using OCR technology that extracts structured data into IRS-approved formats (e.g., XML, JSON, PDF metadata), validated for accuracy through Quality Assurance Reviews that compare digital output to the original paper submission, and the digitized files are securely transmitted to IRS systems (e.g., MeF, IRIS, GMF, etc.) via encrypted electronic file transfer.

C. How the Data Is Stored - The information will be temporarily stored in encrypted, access-controlled environments that meet IRS Publication 4812 and FedRAMP High security requirements. While being stored for up to 60 days following IRS validation, all paper remains secured in locked containers compliant with IRA and NARA standards.

D. How the Data Is Secured - Strict administrative, technical, and physical safeguards, including background investigations, role-based access controls, audit logging, encryption, and NIST-compliant destruction procedures, are used to protect PII and Federal Tax Information throughout its lifecycle. In addition, the contractors do not independently analyze or retain the data beyond what is required to fulfill IRS-directed processing and validation.
Administrative Controls
• Moderate background investigations for all personnel
• Staff-Like Access approval by IRS Personnel Security
• Annual Security Awareness Training (SAT) and UNAX certification
• Written Quality Control and Incident Response procedures
• Compliance with IRS Publication 4812 and IRM 10.5.1

Technical Controls
• Encryption of data in transit and at rest
• FedRAMP High cloud security standards (by Jan 1, 2026)
• Firewall, intrusion detection, and access logging
• Multi-factor authentication where applicable
• Secure file transfer protocols
• Daily audit log retention in IRS-approved formats

Physical Controls
• NARA-compliant facilities
• Access-controlled workspaces
• Double packaging and labeling of shipments

• Secure remittance containers
• NIST SP 800-88 compliant shredding for destruction

25 Is any data accessed, processed and/or stored outside the United States or US Territories?

No

26 Describe the procedures for agency oversight on contractor, access, storage, and destruction of PII, disclosure awareness training and incident reporting.

Note: This question will be revised, and I was asked to address the following questions as a replacement to Q26:

A. What procedures does the agency use to oversee the contractor's authorized access to PII?

The IRS oversees contractor access to PII through a layered authorization and monitoring process:

• Staff-Like Access Determination: All contractor personnel must undergo background investigations and suitability determinations conducted by IRS Personnel Security prior to handling PII
• HSPD-12 / PIV Credentialing: Contractors requiring facility or system access must obtain appropriate credentials
• Role-Based Access Controls (RBAC): Access to systems and data is limited strictly to personnel whose duties require it
• Contracting Officer (CO) and COR Oversight: The CO and COR monitor compliance with contractual privacy and security requirements
• Audit Logs & Access Monitoring: Contractor systems must generate audit logs tracking who accessed PII, when, and for what purpose
• IRS Cybersecurity Oversight: The IRS Cybersecurity Office reviews security architecture, system controls, and FedRAMP compliance

B. How does the agency ensure the contractor properly safeguards and stores PII?

The IRS ensures proper safeguarding through contractual, technical, and operational controls:

• Publication 4812 Compliance: Contractors must adhere to IRS Publication 4812, which governs security and privacy controls
• FedRAMP High Requirement: Contractor cloud environments must meet FedRAMP High security standards (by January 1, 2026)
• Encryption: Data must be encrypted in transit and at rest (secure electronic file transfers that are monitored and encrypted)
• Physical Safeguards: NARA-compliant facilities; secure containers; double-packaged shipping; controlled facility access; post-scanning burn bags and shred boxes are secure, sealed, opaque containers; if not in the vendors' custody, burn bags and/or shred boxes must be stored within a Sensitive Compartmented Information Facility (SCIF) or security-approved open storage area pending collection by authorized personnel; Contractors must maintain waste material in a secured (locked) container in a secured area

• Quality Assurance Surveillance Plan (QASP) for each vendor: The IRS monitors performance and compliance with safeguarding standards; vendors are evaluated annually
• Periodic Reviews and Inspections: The IRS reserves the right to inspect contractor facilities and processes; CORs will periodically review work areas to ensure that contractors are discarding sensitive waste material properly; CORs will conduct periodic unannounced inspections at the off-site contractor facilities (including cloud service providers) where contractors handle IRS SBU data
• Segregation of Duties: Contractor processes must prevent unauthorized viewing or alteration of PII

C. What procedures are in place to oversee the contractor's disposal or destruction of PII?
The IRS enforces strict destruction oversight procedures:
• Paper Retention Controls: Paper documents must be retained up to 60 days post-IRS validation before destruction
• Quality Assurance Review (QAR) Completion Requirement: No destruction may occur until both Contractor Quality Assurance Review and IRS validation are complete
QAR standards for Disposal of Scanned Documents
(1) After all documents have completed scanning and quality control, ensure that the documents are securely moved and maintained in temporary storage.
(2) The cases need to be maintained in date order. Each box contains information indicating the number of documents included.
(3) Documents are retained in temporary storage for a minimum of 14 business days before disposal after acknowledgement of Form 15408-A.

For temporary storage, while waiting for destruction of sensitive waste, it is not necessary to put documents in a locked receptacle if the requirements for burn bags or shred boxes are as follows:
a) SBU data to be destroyed may be torn and placed 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.
• NIST SP 800-88 Compliance: Destruction must meet federal media sanitization standards
• Documented Destruction Confirmation: Contractors must provide written confirmation of shredding/degaussing, including date, time, and equipment details
• IRM & Publication Compliance: Destruction must align with the Standard Operating Procedures for the Disposal of Digitized/Digitalized Paper Records, Guidelines for Industry Partners (GIP), IRM 10.5.6, IRM 11.3.24, and Publication 4812

• IRS Inspection Authority: The IRS may inspect facilities and destruction procedures

D. How does the agency ensure the contractor completes required PII disclosure awareness training?
The IRS requires and verifies mandatory training compliance:
• Annual Security Awareness Training (SAT): Contractors must complete IRS-approved SAT modules annually
• UNAX Certification: Contractors must complete Unauthorized Access (UNAX) awareness training
• Form 14616 Certification: Contractors must certify completion of security awareness training
• COR Monitoring: The COR tracks training certification status
• Staff-Like Access Dependency: Access to IRS systems or data may be revoked if training requirements are not met

E. What procedures does the agency use to oversee contractor incident reporting involving PII? The IRS enforces formal incident reporting and response protocols:
• Immediate Reporting Requirement: Contractors must notify the IRS immediately upon discovery of any suspected or confirmed compromise
• OMB 17-12 Compliance: Incidents must follow federal breach reporting standards
• Publication 4812 Incident Procedures: Contractors must adhere to IRS incident response requirements
• Audit Log Retention: Contractors must maintain and provide audit logs to support investigations
• IRS Cybersecurity Coordination: The IRS Cybersecurity Office reviews incidents and directs remediation actions
• Corrective Action & Documentation: Contractors must document mitigation steps and may be subject to contractual remedies or penalties
• Continuous Monitoring: The IRS monitors compliance through QASP and performance reporting

27 If applicable, what is the IRS PCLIA Number for the system that is providing the information associated with this contract?
2263

28 Are you receiving only the data that is needed to accomplish the task?
Yes

29 From what sources are you obtaining data (other than the IRS) to fulfill this contract?
Not Applicable - The contractors do not obtain data from any external sources to fulfill this contract.

30 Do you have subcontractors who work on the contract?
Yes

30.1 What is the subcontractor's name(s)?
[XX XX X]

30.2 Who is the subcontractor point(s) of contact?
XX XX

30.3 What is the subcontractor email address(es)?
XX XX X

30.4 What is the subcontractor phone number?
XX XX X

30.5 What are the services provided by the subcontractor(s)?
[XX XX X]

30.6 What PII/SBU data is shared with the subcontractor?
Address, Agency Sensitive Information, Employer Identification Number, Employment Information, Name, Protected Information, Social Security Number (including masked or last four digits), Tax ID Number, Telephone Numbers

30.7 Are you sending only the data that is needed to accomplish the task?
Yes

31 Does this system use Artificial Intelligence (AI)?
Yes

32 Does the system use cloud computing?
Yes

32.1 Please identify the Cloud Service Provider (CSP).
Iron Mountain InSight

32.2 Is the CSP FedRAMP Authorized?
No

32.3 Privacy laws (including access and ownership) can differ in other countries. Does the data physically reside in systems located in the United States and its territories and is all access and support of this system performed from within the United States and its territories?
Yes

33 Who owns and operates the system (IRS Owned and Contractor Operated, Contractor Owned and Operated)?

Contractor Owned and Operated scanning systems with fully compliant OCR LLM-AI, and cloud computing environments; IRS Owned and Operated ingestion systems (MeF, IRIS, AIR, GMF, FATCA, CSS).

33.1 Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)?

Yes

34 Identify the roles and their access level to the PII data. Indicate whether background investigations are complete or not.

Under the ZPI Digitalization-as-a-Service (DaaS) contract, access to PII and Federal Tax Information (FTI) is strictly role-based and limited to personnel with authorized Staff-Like Access approval. All contractor personnel handling PII must undergo IRS background investigations and complete required training prior to access. All access is granted under the principle of least privilege. Access is limited strictly to what is required to perform assigned duties. Role-based access controls (RBAC) enforce separation of duties. Audit logs track all access and processing activity. No contractor personnel are authorized to access PII without proper vetting and approval. For all contractor personnel with access to PII, background investigations must be completed or interim Staff-Like Access approved prior to handling PII. Access may be revoked if suitability conditions change.

A. Technical Development Lead (TL)

• Access Level:
o Limited operational access to PII within processing systems
o Access to quality reports, dashboards, and performance metrics
o May view PII only as necessary to resolve processing or system issues
• Purpose of Access:
o Oversight of contract performance
o Coordination with IRS Lead Responsible Engineer
o Issue resolution and compliance monitoring
• Background Investigation Status:
o Moderate Risk Background Investigation required o Staff-Like Access determination required prior to access
o Annual Security Awareness and UNAX training required

B. Scanning & Extraction Operators

• Access Level:
o Access to physical paper submissions
o Access to scanned document images
o No authority to alter IRS system records beyond extraction process
• Purpose of Access:
o Scanning documents
o Capturing images

o Running OCR/ICR extraction
• Background Investigation Status:
o Moderate Risk Background Investigation required
o Staff-Like Access approval required before handling SBU/FTI
o Annual SAT and UNAX certification required

C. Quality Assurance Review (QAR) Personnel
• Access Level:
o Access to original paper submissions
o Access to extracted XML metadata
o Authority to compare, verify, and document discrepancies
• Purpose of Access:
o Conduct required 10% sampling review
o Validate field-level accuracy
o Confirm compliance prior to destruction
• Background Investigation Status:
o Moderate Risk Background Investigation required
o Staff-Like Access determination required
o Annual privacy and security training required

D. Payment Processing Personnel
• Access Level:
o Access to check and remittance data
o Access to bank routing/account numbers
o Limited handling of discovered remittances (cash, etc.)
• Purpose of Access:
o Digitize and transmit remittance information
o Meet statutory payment timelines
• Background Investigation Status:
o Moderate Risk Background Investigation required
o Staff-Like Access approval required
o Additional controls for remittance handling

E. System Administrators (Contractor IT Personnel)
• Access Level:
o Elevated system-level access
o Potential access to encrypted PII repositories
o No business use of PII beyond system maintenance
• Purpose of Access:
o Maintain scanning systems
o Ensure encryption, logging, and transmission functionality
o Support incident response
• Background Investigation Status:
o Moderate Risk Background Investigation required (or higher if designated)
o Staff-Like Access approval required
o Subject to enhanced monitoring and audit logging

F. IRS COR / Oversight Personnel
• Access Level:
o Oversight access to reports and dashboards
o Access to sample documentation for validation purposes
• Purpose of Access:
o Monitor contractor compliance
o Validate deliverables
o Conduct quality assurance oversight
• Background Investigation Status:
o Federal employee clearance per IRS standards

35 Describe the system's audit trail in detail.

The system maintains a comprehensive, end-to-end audit trail as a record of contractor handling and digital processing of IRS submissions (paper tax returns, information returns, correspondence, payments). The audit trail covers the full lifecycle of PII and Federal Tax Information (FTI), from physical receipt through digitization, transmission, validation, retention, and destruction. Audit logging is implemented at the application, database, operating system, and network layers to ensure complete accountability and traceability. The audit trail provides full lifecycle accountability in which it can be determined who accessed PII, what actions were taken, when they occurred, what systems were involved, and how the information moved from receipt to IRS ingestion and destruction. Logging controls meet IRS Publication 4812 requirements, align with NIST AU controls, and support FedRAMP High standards for auditability, monitoring, and incident response. The logging strategy provides a comprehensive, controlled, and verifiable audit trail that balances operational traceability with strict protections for PII/SBU/TPI, enabling IRS oversight, quality assurance, and timely incident response while meeting federal privacy and security standards.

36 Does this system use, or plan to use SBU Data in a non-production environment?

No

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

MeF (for tax returns); IRIS, AIR, GMF, FATCA (for info returns & non-tax forms); CSS (for correspondence)

Incoming/Outgoing

Both

Transfer Method

Other

Other Transfer Method
AWS; A2A; EFTU; IEP; Kiteworks; Mail; SDE; SDT; SFTP

Interface Type
Forms
Agency Name
Form 1040 - Individual Income Tax Return
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

Interface Type
Forms
Agency Name
Form 941 - Employer's Quarterly Federal Tax Return
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

Interface Type
Forms
Agency Name
Form 940 - Employer's Annual Federal Unemployment (FUTA) Tax Return
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 34.022 - Automated Background Investigations System (ABIS)
Describe the IRS use and relevance of this SORN.
Contractors require clearance.

SORN Number & Name
IRS 24.046 - Customer Account Data Engine Business Master File
Describe the IRS use and relevance of this SORN.
Contractors will upload digital files to this system of record.

SORN Number & Name

IRS 00.007 - Employee Complaint and Allegation Referral Records

Describe the IRS use and relevance of this SORN.

Current and former IRS contractors may be the subject of TIGTA complaints received by the IRS.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

Contractors digitize the paper records sent to IRS platforms.

SORN Number & Name

IRS 22.061 - Information Return Master File

Describe the IRS use and relevance of this SORN.

Contractors will upload digital files to this system of record.

SORN Number & Name

IRS 34.021 - Personnel Security Investigations

Describe the IRS use and relevance of this SORN.

Contractors require clearance.

SORN Number & Name

IRS 70.001 - Individual Income Tax Returns, Statistics of Income

Describe the IRS use and relevance of this SORN.

Contractors conduct reporting on work being done.

SORN Number & Name

IRS 34.003 - Assignment and Accountability of Personal Property Files

Describe the IRS use and relevance of this SORN.

Contractors have use of government property/GFE.

SORN Number & Name

Treasury .015 - General Information Technology Access Account Records

Describe the IRS use and relevance of this SORN.

Contractors have authorized access to Treasury IT resources.

SORN Number & Name

IRS 34.016 - Security Clearance Files

Describe the IRS use and relevance of this SORN.

Contractors require clearance.

SORN Number & Name

IRS 10.004 - Stakeholder Relationship Management and Subject Files

Describe the IRS use and relevance of this SORN.

Contractors are individuals who have stakeholder relationships with the IRS.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GRS 3.2 - Information Systems Security Records

What is the GRS/RCS Item Number?

031

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

System access records. These records are created as part of the user identification and authorization process to gain access to systems.

What is the disposition schedule?

Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

Data Locations

What type of site is this?

Data Gateway

What is the name of the Data Gateway?

Vendor Reporting SharePoint Site

Please provide a brief description of the Data Gateway.

Reporting SharePoint site with performance reporting/tracking and no PII.

What are the incoming connections to this Data Gateway?

SLA from vendors' GFE to report on performance metrics being tracked by IRS (no PII).

What are the outgoing connections from this Data Gateway?

Accessed via SLA from vendors' GFE to monitor reports on performance metrics being tracked by IRS (no PII).