Date of Approval: 08/23/2024
Questionnaire Number: 1529

Basic Information/Executive Summary

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

Media and Publications - 2024 Individual Taxpayers Survey

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.

Media and Publications (M&P) Division of the Internal Revenue Service measures external customer satisfaction with its products and services to enhance taxpayer's abilities to understand and meet federal tax obligations. Survey feedback is critical to assess customers' perception of IRS products and services. The Individual Taxpayers Survey is specifically designed to gather taxpayer satisfaction and experience with key tax products (print and electronic versions of forms and publications) and services the IRS offers for federal tax preparation. Questions also ask about taxpayers' experiences with the IRS website and request suggestions to make preparing and filing taxes easier. The Individual Taxpayers Survey is administered through the US postal mail along with an option to complete the survey via a secure online platform. Surveys are conducted annually at the end of filing season, and benefits to the IRS include: 1. Assessing the level of customer satisfaction with M&P's products and services 2. Providing M&P with suggestions for product and service improvements 3. Producing actionable results used to improve specific products and business processes 4. Generating an

understanding of customer satisfaction with all aspects of a tax product (e.g., ease of use, readability, clarity of language) Upon request, survey reports may be shared with the Treasury Inspector General for Tax Administration (TIGTA) and the Taxpayer Experience Office (TXO), which has oversight and responsibilities with customer experience surveys (CXS).

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).

PII is used to select and recruit participants. Postal addresses are used for recruitment. Participants for the Individual Taxpayers Survey are selected from an existing Compliance Data Warehouse (CDW) database of federal tax returns and recruited via postal mail. The contractor assigns a unique identification number to each volunteer in the sample to replace names, addresses, or other personally identifiable information. Although the contractor can match responses to an individual taxpayer using the identifier, the purpose of the research and IRS Disclosure and Security guidelines prohibit the contractor from identifying individual taxpayers who participate in the survey or in reports. The contractor deletes all PII from the data retained. Only aggregated data are used in analysis and reporting sent to the Business Unit (BU). Sensitive data are transferred between the contractor and the IRS as secured, encrypted, and zipped electronic files via the Enterprise File Transfer Utility (EFTU) process, and the passphrase to open the files is communicated separately via an alternate method (e.g., email or phone call). All records will be deleted or destroyed in accordance with approved retention periods. Records will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS General Records Schedule (GRS) 6.5, Item 010 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. GRS may be superseded by IRS specific RCS in the future.

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

Address
Federal Tax Information (FTI)
Name

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

Product Information (Questions)

1.1 Is this survey a result of the Inflation Reduction Act (IRA)?
No

1.13 What is your research method(s) used (i.e., survey, telephone interview, focus group, etc.)?
Survey and Focus group

1.14 Is this a new survey, telephone interview, focus group, or usability testing? Throughout the rest of this questionnaire, we will use the term "survey" to include all of these.
No

1.15 Is there a Privacy and Civil Liberties Impact Assessment (PCLIA) for this survey?
Yes

1.16 Enter the full name of the most recent PCLIA.
2021 External Customer Satisfaction Survey

1.17 Enter the PCLIA number of the most recent PCLIA.
5961

1.18 What are the reasons for the change?
Redesigned survey questions. In prior years, this survey was combined with three other M&P surveys, Individual Taxpayers, Business Taxpayers, and Forms Distribution Surveys; however, SOI requested all four surveys be separated and required four individual submissions for Privacy Act and Paperwork Reduction Act clearance.

1.19 Which Business Unit (BU) is requesting this survey?
Taxpayer Services, Media and Publications

1.21 Who will the survey be administered to?
An external survey administered to Individual Taxpayers.

1.22 What is the start date?
8/7/24

1.22 Is this a reoccurring survey?

Yes

1.22 Will the survey be administered annually (3-year expiration)?

Yes

1.23 What is the end date?

8/7/27

2.11 Will the survey capture any type of PII or is PII (names, addresses, email addresses, etc.) used to select participants?

Yes

2.12 If any PII data is collected, disclosed, or studied on individuals who choose not to participate, please describe the data.

No

2.13 List any linkable data that the survey uses, collects, receives, displays, stores, maintains, or disseminates (gender, ethnicity, parts of address, tax filing information, etc.) or uses to select participants?

Name, Address, and Federal Tax Information.

2.14 Explain how the participants are selected. Include a detailed description. Please provide your research plan as supporting documentation.

The sample for the M&P Individual Taxpayers Survey is a simple random sample drawn from customer cases in the respective sampling frame/population: taxpayers who filed a federal income tax return in the processing year of interest. Taxpayer Services, Strategies and Solutions (TSSS) pulls and prepares these samples. Participants are randomly selected from the CDW database Individual Master File (IMF). M&P sets sample size for the individual taxpayer sample. The Individual Taxpayers Survey excludes records with an invalid mailing address, international or military addresses, deceased taxpayers, and duplicate records.

2.15 How are the participants notified (letter, postcard, email, etc.) of the survey, and if the survey is voluntary/optional, how is notice given? If it is not voluntary, please explain why it is mandatory.

Participants in the Individual Taxpayers Survey are notified of the survey by postal mail. Notice of participation as voluntary/optional is provided in the recruitment letter, survey, and reminder letters.

3.11 What tool(s) is/are used to conduct the survey? Please indicate if the anonymous feature has been set for the survey, if applicable.

The contractor uses Qualtrics, a FedRAMP certified data-collection survey tool to create and conduct the survey. The anonymous feature is set for the survey.

3.12 Will the survey be audio-recorded or video-recorded?

No

4.11 Does this survey retrieve information by any personal identifier for an individual who is a U.S. citizen, or an alien lawfully admitted for permanent residence? If the answer is Yes, you must have at least one SORN name and number selected in the SORNs section.

Yes

4.12 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records to inform each individual requested to supply information about themselves. Do survey participants provide information about themselves?

Yes

4.13 Please provide the Privacy Act Statement.

Our authority for requesting information with this survey is 5 U.S.C. Section 301, and 26 U.S.C. Sections 7801, 7803, and 7805. The information you provide allows the IRS to analyze interactions between the IRS and taxpayers. This information will also help us to improve taxpayer services. Data collected will be shared with IRS staff, but your responses will be used for research and aggregate reporting purposes. The information you provide will be protected as required by law. We estimate it will take 15 minutes to complete this survey, including the time for reviewing instructions and completing the collection of information. Providing the information is voluntary; not providing all or part of the information requested will have no impact on you but may reduce our ability to address concerns with IRS tax products and services. We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB control number. The OMB number for this survey is 1545-1432. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to: IRS, Special Services Section, C:DC:CAR:MP:T, Room 6129, 1111 Constitution Avenue, NW, Washington, DC 20224.

4.14 Does the IRS administer (conduct) the survey?

No

4.21 If a contractor administers (conducts) and analyzes the survey, is all work performed and contained in the United States?

Yes

4.22 How does the administrator of the survey protect employees' or taxpayers' SBU/PII from compromise, loss, theft, or disclosure?

Whenever information is stored on IT assets at the contractor’s facility, the contractor must be compliant with the National Institute of Standards and

Technology (NIST) SP 800-53, Recommended Security Controls for Federal Information Systems & Organizations controls. Specific practices utilized by the contractor include encrypting all data when at rest and in transit following approved encryption standards and methods, classifying all data for proper storage, employing role-based access control to ensure only those with a business need and with proper background clearance have access to the data, and ensuring all remote access uses a two-factor authenticated FIPS 140 compliant VPN. The contractor will process and store all data in the FedRAMP authorized Microsoft Azure Government cloud environment. The contractor validates Microsoft's ongoing compliance with FedRAMP authorization requirements to enforce physical security requirements for securing data under NIST SP 800-53. Only authorized contractor employees will have access to the data and will adhere to IRS guidance to ensure any PII data are not compromised, lost, stolen, or disclosed. While survey data the contractor provides the IRS will not contain any PII data, the files will also be securely stored on an encrypted IRS server.

4.23 Where and how is the PII stored and protected?

All PII data will be safeguarded using protocols in keeping with IRS Publication 4812. Data is collected to an Excel spreadsheet, and a unique number is assigned to each record to protect PII. Data will be stored on the contractor's FedRAMP certified Microsoft Azure Government cloud environment. The contractor staff with access to the data have proper background clearance. Additionally, when analyzing and transmitting findings, all PII is removed from individual records.

4.24 Provide the Cyber Security approved security and encryption used when data is transferred electronically from the IRS to contractors and back to the IRS.

Data is transferred between the contractor and the IRS as a secured, encrypted, and zipped electronic file via the IRS Enterprise File Transfer Utility (EFTU) process. Cyber Security and National Institute of Standards and Technology (NIST) require data be transferred via password-protected encrypted disk via FedEx overnight mail (including return acknowledgement form), through EFTU, or using the Secure Zip data transfer method. Although EFTU and Secure Zip are preferred, currently all methods are being used.

4.25 How is the survey PII protected and stored when it is housed at a contractor site on contractor computers? Provide a detailed explanation of the physical and electronic security and protection of the data before, during and after the survey.

The contractor uses Qualtrics, a FedRAMP certified, data-collection and survey development tool and stores data on the contractor's secure Microsoft Azure Government cloud server. During the survey, the contractor assigns a unique identification number to each record included in the sample. This unique identifier replaces names, addresses, or other personally identifiable information. Although the contractor can match responses to a participant using the unique identifier, due to the purpose of the research and IRS Disclosure and Security guidelines, the contractor will not identify participants in the survey or reports. Information that can identify a participant is deleted from the data retained by the contractor. Only

aggregated data is used in analysis and reporting sent to the Business Unit (BU). Once the aggregated data is sent to the BU, the original data is then destroyed. Data housed at the contractor site are required to be segregated from other non-IRS data, and all data at rest or in transport must be encrypted. Whenever information is stored on IT assets at the facility, the contractor must be compliant with the implementation of NIST 800-53, Recommended Security Controls for Federal Information Systems & Organizations controls. All data with PII will be safeguarded using protocols in keeping with IRS Publication 4812. The contractor's staff with access to the data have suitability clearance. Additionally, when analyzing and transmitting findings, all PII will be removed from individual records and datasets. Data is transferred between the contractor and the IRS as a secured, encrypted, and zipped electronic file via Enterprise File Transfer Utility (EFTU) process. The contractor's procedures ensure strict protection of access to and use of all research data, mandate systematic physical and logical access control, as well as explicitly define security policy and procedures governing media access, server security, sensitive data handling, audit and accountability, router security, and the prevention of unauthorized access. As standard procedure, all research data is stored in a secure network of servers protected by a firewall and located in a secured, locked room. Access to the data center is restricted to authorized persons and alarms are monitored 24x7x365. Annually since 2011, the contractor has passed on-site IRS security review, indicating compliance with the requirements of NIST 800-53, Revision 3, Annex. All records related to names and contact information used for recruiting and survey participation will be verifiably destroyed once used.

4.26 Has a Contracting Officer or Contracting Officer's Representative (COR) verified the contract included privacy and security clauses for data protection and that all contractors have signed non-disclosure agreements which are on file with the COR?

Yes

4.27 Identify the roles and their access level to the PII data.

Contractor Users Read and Write
Contractor Managers Read and Write
Contractor Developers Read and Write
Contractor Sys. Admin Read and Write

4.28 Explain the precautions taken to ensure the survey results will not be used for any other purpose not listed in the Detailed Business Purpose and Need section and to ensure that employees or taxpayers who participate in the survey cannot be identified or re-identified under any circumstances and no adverse actions taken.

Survey participants cannot be identified or re-identified, and no adverse actions can be taken against participants because their identities are unknown. The contractor will not include PII in survey data files and reports provided to the IRS. Additionally, due to the purpose of the research and IRS Disclosure and Security guidelines, data is destroyed one year after resolved, or when no longer needed for business use, whichever is appropriate.

4.28 Identify the roles and their access level to the PII data and indicate whether their background investigation is complete or not.

Contractor Users Read and Write High Yes Contractor Managers Read and Write High Yes Contractor Developers Read and Write High Yes Contractor Sys. Admin Read and Write High Yes

4.29 Does the administrator of the survey have access to information identifying participants?

Yes

5.11 For employee or taxpayer satisfaction surveys explain how you have ensured that no "raw" or unaggregated employee or taxpayer data will be provided to any IRS office.

No raw or unaggregated data will be provided to the IRS. During the survey, the contractor assigns a unique identification number to each participant in the sample. This unique identifier replaces names, addresses, emails or other PII. The contractor sends the data files without PII, and taxpayer information cannot be linked to the participant. All collected data, including any PII data used to pull the sample, will be securely stored on the contractor's Microsoft Azure Government Cloud server--an encrypted FedRAMP compliant platform.

5.13 Does the individual about whom the information was collected or maintained expressly authorize its collection/maintenance?

Yes

Interfaces

Interface Type

Other Federal Agencies

Agency Name

Taxpayer Experience Office (TXO)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Secure email/Zixmail

Interface Type

IRS Systems, file, or database

Agency Name

Compliance Data Warehouse (CDW)

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Other

Other Transfer Method
Sybase IQ (data access language) used to access CDW data and EFTU used to send data to contractor.

Interface Type
IRS or Treasury Contractor
Agency Name
XXXXX
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
IRS or Treasury Contractor
Agency Name
XXXXX
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Direct input by participants.

Interface Type
Other Federal Agencies
Agency Name
Treasury Inspector General for Tax Administration (TIGTA)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Secure email/Zixmail

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 24.046 - Customer Account Data Engine Business Master File
Describe the IRS use and relevance of this SORN.
To access tax records for each applicable tax year or period, including employment tax returns, partnership returns, excise tax returns, retirement and employee plan returns, wagering returns, estate tax returns, information returns, representative authorization information, and Device ID.

SORN Number & Name

IRS 00.001 - Correspondence Files and Correspondence Control Files

Describe the IRS use and relevance of this SORN.

To track correspondence including responses from voluntary surveys.

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

To access tax records for each applicable tax period or year, representative authorization information (including Centralized Authorization Files) of any taxpayer's account.

SORN Number & Name

IRS 00.003 - Taxpayer Advocate Service and Customer Feedback and Survey Records

Describe the IRS use and relevance of this SORN.

To improve quality of service by tracking customer feedback (including complaints and compliments), and to analyze trends and to take corrective action on systemic problems.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

To identify and track any unauthorized accesses to SBU and potential breaches or unauthorized disclosures of such information or inappropriate use of government computers to access Internet sites for any purpose forbidden by IRS policy (e.g., gambling, playing computer games, or engaging in illegal activity), or to detect electronic communications sent using IRS systems in violation of IRS security policy.

SORN Number & Name

IRS 22.062 - Electronic Filing Records

Describe the IRS use and relevance of this SORN.

Electronic return providers (electronic return preparers, electronic return collectors, electronic return originators, electronic filing transmitters, individual filing software developers) who have applied to participate, are participating, or have been rejected, expelled or suspended from participation, in the electronic filing program.

Records Retention

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
Public Customer Service Records
What is the GRS/RCS Item Number?
6.5
What type of Records is this for?
Both (Paper and Electronic)
Please provide a brief description of the chosen GRS or RCS item.
Evaluations and feedback about customer services. All records will be deleted or destroyed in accordance with approved retention periods. Any records will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS General Records Schedule (GRS) 6.5, Item 010 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. GRS may be superseded by IRS specific RCS in the future.
What is the disposition schedule?
Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

Data Locations

What type of site is this?
Data Gateway
What is the name of the Data Gateway?
Compliance Data Warehouse (CDW)
What is the sensitivity of the Data Gateway?
Federal Tax Information (FTI)
What is the URL of the item, if applicable?
https://cdw.web.irs.gov
Please provide a brief description of the Data Gateway.
The CDW database hosts detailed federal tax returns metadata on an accessible website. Access to CDW is controlled by the IRS Business Entitlement Access Request System (BEARS). Users request the level of access based on their business need. Masked data access - which does not include PII - requires the approval of their manager of record. Access to unmasked data - which includes PII - requires the approval of their manager of record as well as a BOD-designated executive. CDW also hosts some restricted data sets which require additional approval of the data owner prior to

access being granted. Access is highly restricted to preserve system functionality and security.

What are the incoming connections to this Data Gateway?

Sybase IQ software provides a toolkit for creating, editing, and submitting Structured Query Language (SQL) statements to CDW databases. The package includes the Open Database Connectivity (ODBC) driver for Sybase IQ, which is essential for using other data analysis tools to access data in CDW.

What are the outgoing connections from this Data Gateway?

Data is retrieved from the CDW database using the Sybase IQ tool and Structured Query Language (SQL) program tool. Results are saved and stored as an Excel or Statistical Program for the Social Sciences (SPSS) file on a secure IRS network drive (\wi_research2\CARE Surveys\MP), and each project is stored in a separate folder. Only IRS analysts working on the project and with proper clearances can access the data. Data shared with project contractors are transmitted using the IRS secure EFTU system. The contractor stores data on their secure Microsoft Azure Government cloud-base environment (see https://marketplace.fedramp.gov/products/F1603087869), and uses Qualtrics, a FedRAMP-certified, cloud-base environment (see https://marketplace.fedramp.gov/products/ F1606097904) to conduct data analyses and produce aggregate reports.

What type of site is this?

System

What is the name of the System?

Qualtrics survey tool (contractor)

What is the URL of the item, if applicable?

Contractor secured data site.

Please provide a brief description of the System.

System is a designated survey results folder.

What are the incoming connections to this System?

The Qualtrics Survey tool receives survey responses directly from the participant; the data gets analyzed and aggregated in the tool to generate the report.

What are the outgoing connections from this System?

Aggregated reports without PII associated to the individual are distributed to clients (Media and Publications) as an email attachment.

What type of site is this?

Shared Drive

What is the name of the Shared Drive?

CustSatReporting

What is the URL of the item, if applicable?

\wi_research2\CARE Surveys\MP

Please provide a brief description of the Shared Drive.

Data is stored as an Excel or Statistical Program for the Social Sciences (SPSS) file on a secure IRS Taxpayer Services network drive, and each project is stored in a separate folder. Only IRS analysts assigned to the project and with proper clearances can access the data.

What are the incoming connections to this Shared Drive?

Data is saved and stored as Excel or Statistical Program for the Social Sciences (SPSS) files and reports as Microsoft Word documents on a secure IRS Taxpayer Services network drive, and each project is stored in a separate folder. Only IRS analysts assigned to the project and with proper clearances can access the data.

What are the outgoing connections from this Shared Drive?

Aggregated reports without PII are distributed to clients (Media and Publications) via email.