Date of Approval: **September 14, 2023**

PIA ID Number: **6883**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Augmented Reality Pilot, AR

Is this a new system?

Yes

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Enterprise Case Management (ECM) Executive Steering Committee, Enterprise Digitalization Integration Board (DIB)

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The Augmented Reality pilot, also known as the InFORM Me mobile application, is currently a proof-of-concept effort. InFORM Me has augmented reality (AR) technologies built-in and embedded into the application, which is used in features such as the Document Scanner. The application is still in early development and only a prototype is currently in scope. The InFORM me system/application will improve the taxpayers' experience in navigating different tax issues in a more modern and interactive solution. The application's use of artificial intelligence and machine learning, makes the process quicker and easier which eliminates taxpayers' frustrations and mitigates the need to call the IRS hotline. The application allows the end user to search for and interact with the InFORM Me virtual tax assistant (chat feature) to help the user find all related information for what they requested information on; ultimately this improves tax compliance and improves the taxpayers understanding of their tax responsibilities. The application allows the public user, or taxpayer, to voluntarily download the InFORM Me application on their mobile device(s) (running iOS or Android). They can build a profile using the profile builder which will, along with their search criteria, further assist the artificial intelligence to learn what is most

relevant and generate more relative and comprehensive returns of information. The InFORM Me application allows for other self-help activities, such as the use of camera scans of tax forms through the use of their device. Direct access to digital forms within the application enables users to learn about any line item on the form. When needed, the application can redirect the user to IRS.gov or the IRS2GO mobile application, providing that application is also installed on their mobile device. Any PII contained in the InFORM Me application will be blocked/redacted, and notifications will be personalized throughout the user's journey. The InFORM Me application further supports the IRS mission to provide an efficient and compliant integration with IRS sites with the use of Augmented Reality (AR) and to improve taxpayer(s) experience and reduce potential call volumes.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e., last 4 digits, etc.)?

No

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing Address
Internet Protocol Address (IP Address)
Employment Information
Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Protected Information - Information which if modified, destroyed, or disclosed in an unauthorized manner could cause loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

When completing the Profile questions, the end user indicates whether they're: Individual or Business Type of filer: Student, Parent, Military, Senior, Self-Employed, Gig worker, Employee Filing status: Single, Married Filing Joint, Married Filing Separate, Head of Household, Widower Has dependents or not State Age range: Under 65 or older Citizenship Status In the chat feature, unsolicited SBU may be entered by the end user, but the application will block this data.

Cite the authority for collecting SBU/PII (including SSN if relevant).

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The InFORM Me application is not a system of storage; therefore, it does not collect or store any PII. The use of SBU/PII is not required, however the potential input of SBU/PII does allow the profile builder to perform its intended function. This data is specific to the device and is user-built by responding to questions related to their tax filing status and/or relational or marital status. This data helps facilitate searches and the information provided aids the user in easily locating and accessing information specific to their self-identified tax (compliance) issue(s). If a user scans their personal tax form or shares unsolicited SBU/PII, with the automated chatbot, in the form of an SSN, the information will be blocked/redacted so that no information can be seen, and no information will show. The application utilizes a script that identifies PII such as phone number, SSN, DOB, etc. and once identified the information is blocked completely on the frontend. On the backend, the information is removed from the user's question. This information allows for the application to aid the user's specific needs. For example, if the user is a gig worker the application will show help tailored to their filing requirements. The application does not collect or store any PII. If the end user scans their personal tax form or shares unsolicited SBU with the automated chatbot, the information is blocked/redacted.

How is the SBU/PII verified for accuracy, timeliness, and completion?

The SBU/PII information is received directly from the end user. It is deemed reliable and accurate. The information is not altered in any way. There is not a business need to verify accuracy, since we are using publicly available data on IRS.gov. Automations are in place to review and update information when changes are detected on IRS.gov.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.037 Audit Trail and Security Records

IRS 00.001 Correspondence Files and Correspondence Control Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

No

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

Yes

Identify the contractor source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: INADEV
Transmission Method: Secure Data Transfer
ISA/MOU: No

Identify the authority.

The authority to disclose information is 6103(n).

For what purpose?

Disclosure to contractors to obtain services that support tax administration.

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?

No

Explain:

No clause is required as no SBU/PII is used or maintained within this application (this is a service-to-build contract).

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

Yes

Briefly explain how the system uses the referenced technology.

Scanning technology uses mobile device camera live feed to identify a form that may contain SBU/PII, but the systems does not collect or read user populated data. The forms to be detected are configured in the backend system along with the fields/widgets that appear on the form. For example: Form 1040, contains a field "filing status" that is configured in the backend system along with its field "filing status", the data for which is gathered by crawling irs.gov website. The OCR (optical character recognition) technology detects the pre-configured form elements related to the identification of the form's fields and widgets. The camera is not used to capture/store any images.

Does the system use cloud computing?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

No

Please explain:

AWS cloud tool is FedRAMP certified. The ATO process will inherit the FedRAMP certification for AWS from JAB (Joint Authorization Board).

Please identify the ownership of the CSP data.

Third Party

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

3rd Party

What is the background check level required for CSP?

None

Is there a breach/incident plan on file?

No

When will Breach/Incident plan be available?

12/31/2024

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Troubleshooting

Does this system/application interact with the public?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Not Applicable

Please explain.

Received the following confirmation from DIRA Team: "No DIRA Required: The InFORM Me Augmented Reality Project from Enterprise Digitalization will be a public-facing application, however, will not require external users to ID Proof and/or Authenticate. Therefore, a DIRA is not required." Confirmation to be uploaded in related documents.

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

The following privacy policy statement will be contained in the application: "You have entered the Internal Revenue Service's website, an official United States Government System. The IRS uses this website to provide information about IRS services and programs. This website includes specific application which provide more services or enable us to respond to specific questions from Web site visitors. We will not collect personal information about you because you visit this Internet site. There are applications on this

website that provide you with the opportunity to order forms, ask questions requiring a response, sign up for electronic newsletters, participate in focus groups and customer surveys, or learn the status of filed returns or anticipated payments. Using these services is voluntary and may require that you provide additional personal information to us. Providing the requested information implies you consent for us to use this data in order to respond to your specific request." The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

The Augmented Reality pilot is currently a proof-of-concept effort. The application is still in early development and only a prototype is currently in scope. If users choose not to scan their personal tax forms, they can use the application dropdown in the form scanner to view and use a blank digital form. Taxpayers are not required to complete the Profile section of the application.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

Publication 1 "Your Rights as a Taxpayer" explains the rights of the taxpayer, which includes the right to challenge the IRS' position and be heard; and the right to appeal an IRS decision in an independent forum. Information is pulled from publicly available information on IRS.gov using automations. The information is then reviewed by the Vendor. The crawler technology is used to crawl and gather content from IRS.gov and the gathered content is stored in the vendor backend system. This content is reviewed/curated for its accuracy and then published to be made available for the mobile application.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated).

Contractor Owned and Operated

The following people have access to the system with the specified rights:

IRS Contractor Employees

Contractor Users: Read Write
Contractor Managers: Read Write
Contractor Developers: Read Write

How is access to SBU/PII determined and by whom?

Only system administrators are granted access.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

All InFORM Me records (including audit/access logs and other system related records) will be preserved using retention, destruction and archiving instructions identified within General Records Schedule (Document 12829) and Records Control Schedule (Document 12990) as approved by NARA. Audit Log Files, General Records Schedule 3.2: Information Systems Security Records (Item 030 and 031) and 3.1 (Item 010, 011, and or 020), Electronic Files - General Records Schedule 5.2: Input Records, Output Records, Electronic Copies (Item 020 - Electronic input/source records,) and 5.2 (Item 020 and 030).

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

No

Describe the system's audit trail.

The system's audit trail is vendor owned and maintained currently. In accordance with FedRAMP, Augmented Reality Initiative, and NIST SP 800-63-3, InFORM Me maintains controls that are capable of producing audit logs for the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Operating systems and component applications (where the capability exists) provide audit logs for audit reports as shown below. Component Auditing Element - Kubernetes, Drupal, Chatbot - Grafana - AWS, MySQL -

CloudTrail, Cloudwatch - Mobile Application - Google Firebase Auditable events listed below are captured on a continuous basis. Audit logs from all components are reviewed at least monthly. Unusual activities of users with significant information systems roles and responsibilities shall be reviewed according to the defined schedule. Also reviewed are historic audit logs in order to determine if a vulnerability has previously been exploited. Unusual activities include failed login attempts, login attempts outside of designated schedules, locked accounts, port sweeps, network activity levels, memory utilization, key file/data access, etc. Access to the audit functionality is provided only to system administrators, developers, and other designated personnel with explicit authorization from the roles they have been assigned. Findings are reported to the system Engineering team and the appropriate stakeholders including designated IRS officials. The selected audit logs are retained by file size specification and retained locally for at least 90 days. Logs are concurrently backed up from CloudTrail into S3 bucket and retained indefinitely. Logs are not altered by administrators, processes, or the operating system. Audit log access is protected by user credentials and role-base access privileges and are read-only files. Audit record time stamps must be recorded with 50 ms precision. Events selected for auditing include 1) Startup and shutdown 2) Loading and unloading of services (only applicable to operating systems) 3) Installation and removal of software (only applicable to operating systems) 4) System alerts and error messages 5) User logon and logoff 6) Administrative activities 7) Modification of privileges and access controls 8) Failed login attempts 9) Changes to passwords or passphrases. The system is not required to generate additional information for the audit records. Auditable events, schedules, and retention are adjusted as needed for compliance to changing law enforcement information, intelligence information, and other credible sources of information. User-installed software events are monitored for compliance weekly. These events have been selected as adequate support for after the fact investigation.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Records are currently stored on Enterprise Digitalization SharePoint under the Augmented Reality project space.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Application is still in active development. Evolving and fixing issues as they occur.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax, or Privacy Act consent?

No