Date of Approval: July 20, 2017 PIA ID Number: **2180**

A. SYSTEM DESCRIPTION

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

2. Is this a new system? Yes

2a. If **no**, is there a PIA for this system?

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Next, enter the **date** of the most recent PIA.

Indicate which of the following changes occurred to require this update (check all that apply).

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
No	Internal Flow or Collection

Were there other system changes not listed above?

If yes, explain what changes were made.

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

A.1 General Business Purpose

5. 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.

IRS is conducting a pilot with ID.me, Inc to explore ID.me's third party "identity-as-a-service" capabilities for improving IRS's identity assurance of taxpayers in remote (e.g. online) interactions.

ID.me is a Federal Identity, Credential and Access Management (FICAM) approved provider. ID.me utilizes the latest technologies outlined in the NIST SP 800-63-2 standards for identity proofing consumers through address of record non-repudiation, user registration, and authentication for Levels of Assurance (LOA3) to include multi-factor authentication credential issuance. ID.me will provide identity verification services for a subset of IRS taxpayers selected for additional identity verification by the taxpayer protection program (TPP). Selected consumers will be asked to authorize the release of NIST 800-63 required identity attributes required by the IRS prior to the release of any information to IRS. The consumer may revoke subsequent access to this information by ID.me or by any relying party at any time by accessing their account settings in ID.me.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
No	Employer Identification Number (EIN)
No	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

The Office of Management and Budget memorandum M-17-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The interaction between ID.me and the IRS Taxpayer Protection Program (TPP) requires the use of SSN to reliably identify the user. However, steps are taken to minimize display and transmissions of the SSN in any form not required to achieve the goals of the program. For this reason, eliminating the use of SSNs is not applicable.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
Yes	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
Yes	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
Yes	Proprietary data	Business information that does not belong to the IRS
No	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

If **yes**, describe the other types of SBU/PII that are applicable to this system.

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

No	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

ID.me will be collecting PII from the consumer as part of the IRS identity verification services pilot. Identity proofing elements, as defined by NIST 800-63, are needed to ensure the consumer's identity can be verified at NIST Level of Assurance 3 (LOA3) as well as provide IRS with requested fraud analysis to identify and deter fraudulent usages of the IRS system. IRS requires a subset of the PII collected during identity verification will be sent to the IRS so IRS can connect the identity proofing attempts with the IRS TPP record and input necessary transaction codes to complete the IRS transaction.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

Taxpayers are notified by mail that they may access this system to verify their identity and will be provided with a disclaimer once they enter the user portal and will be required to accept ID.me Terms or Service and Privacy Policy. The purpose of the IRS system is to verify individuals against NIST 800-63 LOA3 standards for identity proofing consumers through address of record non-repudiation, phone confirmation, fraud checks, user registration, and authentication for Levels of Assurance (LOA3) to include Multi-factor authentication. ID.me verifies accuracy of the transmission of the ate file to IRS via audit logs and encryption capabilities. In order to meet NIST 800-63-2 requirements, the system verifies citizen asserted PII against authoritative records, in this case credit agencies. The system only sends asserted PII and receives verification data from source. ID.me's vendors have non-disclosure (NDA) contracts in place preventing the inclusion of further details in the document.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? No

If **no**, explain why the system does not have a SORN? These are not federal records. They are kept outside the IRS Information Technology boundary and do not require a system of records notification, according to Privacy Act requirements. The records received by IRS are covered under SORNs for the related internal systems.

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. # # Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? No

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Credit and Financial Report Agencies	Secure API	Yes
Document Verification	Secure API	Yes
Mobile Network Operator	Secure API	Yes

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Return Integrity and Compliance Services (RICS)	No		No	

Identify the authority and for what purpose? To RICS via IRS's Secure Data Transfer (SDT) protocol, which is a secure File Transfer Protocol (FTP) process between ID.me servers and IRS servers.

12b. Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. Does this system disseminate SBU/PII to other Sources? Yes

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

Organization Name	Transmission method	ISA/MOU
Credit and Financial Reporting Agencies	Secure API	Yes
Mobile Network Operator	Secure API	Yes
Document Verification	Secure API	Yes

Identify the authority and for what purpose? ID.me transmits data to the IRS to facilitate identifying potential identity theft returns for tax administration purposes.

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

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

    14a. If **yes**, briefly explain how the system uses the referenced technology. Use of mobile, photo and photo of government issued id will be used as part of the identity proofing process

15. Does the system use cloud computing? Yes

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

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

    17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
    The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions. When a return is selected for Examination, Collection etc., the taxpayer is sent the Privacy Act Notice, Your Appeals Rights and How to Prepare a Protest and Overview of

the Appeals Process. As a follow-up on Question 16, above, this system does interact with the public, but does not require an e-RA, because it is outside the IRS Information Technology boundary.

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
All individuals have the right to decline to provide information. However, they may be subject to Examination or Deficiency procedures, at which time they are provided applicable notices, such as Your Appeals Rights and How to Prepare a Protest.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The process and procedures used by the Taxpayer Protection Program are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. As an outside resource, ID.me is not subject to the requirements of "due process" in verifying their identity with ID.me. However, taxpayers in this program are afforded full rights related to IRS tax processing through existing the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process.

I. INFORMATION PROTECTION

20. 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

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

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level(Read Only/Read Write/ Administrator)
Users	No	
Managers	No	
Sys. Administrators	No	
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	No		

21a. How is access to SBU/PII determined and by whom? IRS will not have access to ID.me data directly. The data received from ID.me via IRS SDT will be stored within the TPP systems and IRS users will be required to completed a 5081 to be granted access at the appropriate level. ID.me will not have access to any IRS system and ID.me employees on this project will need to complete all required security training. Per MOA. IRS privacy and security awareness training compliance information is described in IRS publication 1075. Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities. Sections 6.0 and 9.0. Publication 1075 is available at http://www.irs.gov. ID.me employs role-based access controls to servers containing sensitive data. Authorization is done on a least privilege model with access changes requiring ticket and management approval. ID.me personnel is required to complete annual security awareness and privacy training. Consumers who choose to utilize the ID.me identity proofing service and register with the system have access to their own user profile.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act? Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? No

22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

ID.me is unscheduled. The IRS Records Office and system owner will draft and submit to the National Archives a request for records disposition authority. The contractor certifies that the data processed during the pilot/performance of this contract shall be completely purged from all data storage component of his/her computer facility, and no output will be retained by the contractor at the time the IRS work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized inspections or disclosures. At the time the IRS work is completed and statutory obligations of the contractor for minimum data retention periods satisfied, not to exceed 5 years and 60 days, the contractor shall return all IRS data, IRS property, and resulting outputs. The contractor shall then purge all data (including their outputs) from their systems in accordance with NIST SP 800-88 Rev 1 and IRS publication 1075. A Sanitized Validation Form is required to be completed by the individual who performed and verified the destruction. Once completed, the form must be provided to the IRS representative. A sample form can be found in Appendix F of the NIST SP 800-88 Rev 1. Records for the Pilot testing of this system are covered under GRS 3.1 for Technology Management Records, Item 011 System Development Records which covers verification and testing, and are temporary records to be destroyed 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the system s audit trail. The system is a FICAM certified LOA3 process, with a review completed in August 2016, supplemented with the latest techniques outlined in the draft NIST SP 800-63-3. The vendor will also collect a set of attributes for the TPP and share those with IRS through an identified secure process.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 7/24/2017

24.3 If **completed/ or in process,** 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? ID.me is responsible for developing and hosting the application per an MOA with the IRS. ID.me is responsible for providing the source data per the MOA. The MOA will include all the applicable disclosure, retention, safeguards and confidentiality clauses as reviewed and approved by the Office of Disclosure and Procurement. There is a standard UAT plan that is updated as needed based on the changes requested to the site in order to appropriately address privacy requirements. ID.me is a credentialed service provider approved by GSA FICAM and undergoes annual on-site audits against NIST SP 800-63. Logical and physical access controls are required and designed to protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any credential data repositories or credential management processes. Additionally, ID.me monitors and tests controls to ensure they're operating effectively as designed.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees:	Not Applicable
26b. Contractors:	Not Applicable
26c. Members of the Public:	Under 100,000
26d. Other:	No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report