Date of Approval: August 30, 2018 PIA ID Number: **3483**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Information Sharing & Reporting - Sharing, ISR-S

2. Is this a new system? No

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

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

Information Sharing & Reporting - Sharing, ISR-S, 1425, MS5,

Next, enter the **date** of the most recent PIA. 09/23/2015

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

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

Were there other system changes not listed above? No

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
Yes	Detailed Design/Milestone 4A
Yes	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? Yes

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.

The Information Sharing and Reporting - Sharing (ISR-S) project developed an information sharing capability that facilitates the (1) exchange of ACA data between the IRS and Centers for Medicare and Medicaid Services (CMS) systems (as regulated in section 6103 of the Internal Revenue Code), and (2) transfer of ACA data between IRS internal systems, both legacy and ACA (note that all transfers are ACA-related). On Aug.13, 2013, the Internal Revenue Service issued final regulations implementing section 6103(l)(21) of the Internal Revenue Code, as added by the Affordable Care Act (ACA). This provision authorizes the IRS – upon written request and subject to strict privacy and security safeguards – to disclose certain taxpayer information for use in verifying eligibility for health care affordability programs. ISR-S developed over several iterations. Earlier phases facilitated receipt and processing of real-time requests; provided infrastructure services via web services connectivity and service-oriented integration to ACA project systems. ISR-S facilitates the processing of inbound CMS requests and coordinates with internal ACA applications to provide appropriate responses to CMS. The system provides the ability to verify exchange identifiers and family size. For the latest version of ACA, ISR-S connects the legacy system Corporate File On-line (CFOL), to ACA's Information Returns Database (IRDB) database, thus allowing ACA information returns to be viewed by users. In addition, operational metrics will be gathered on this new interface. These metrics will be sent to Enterprise Informatica Platform (EIP) for reporting purposes. ISR-S is unique in that there is no ISR-S application that resides on the component infrastructure. The combined infrastructure components when deployed as ISR-S provide the functionality that ISR-S provides to the rest of the ACA environment. As a result, ISR-S auditing requirements are met through implementing the associated Platform Level Audit Plan(s) and the remaining requirements being identified as part of the ISR-S Audit Plan. Due process is provided pursuant to 26 USC. The E-CLAS release adds a Service Oriented Architecture (SOA)-based scalable Enterprise Services framework for Web services for Core command codes that are currently supported by Consolidated Legacy Access Services (CLAS API)

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 Yes On Spouse Yes On Dependent

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

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
Yes 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-07-16 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The ISR-S system requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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.

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

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
Yes	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.
No	Proprietary data	Business information that does not belong to the IRS
Yes	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

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

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
No	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.

The information is collected for the purpose of complying with a legislative mandate in ACA, in order to (1) conduct tax administration (to determine if tax payers are eligible for health insurance), and (2) provide taxpayer services. ISR-S is critical in supporting the IRS mission to provide enrollment and eligibility determination for federally-mandated health insurance affordability programs. ISR-S processes system-to-system requests between CMS/Health and Human Services (HHS) and ACA systems using SBU/PII identifiers, and between internal IRS systems (both legacy and ACA).

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

Requirements governing the accuracy, timeliness, and completeness of SBU/PII will be such as to ensure fair treatment of all individuals. Information is collected, to the greatest extent practicable, directly from the individual to whom it relates (via taxpayer information submitted directly by the individual who is seeking ACA eligibility). ISR-S serves as a communications conduit between other systems internal and external to the IRS, and does not maintain or verify the SBU/PII data it receives beyond format validation. Determinations based on the SBU/PII data are the responsibilities of systems outside of the scope of ISR-S. There is a process by which taxpayers can amend their returns and other information they provided.

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? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

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? Yes

If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Integrated Enterprise Portal	Yes	12/15/2015	Yes	04/12/2018

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

If **yes**, for each federal interface, identify the organization 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
HHS CMS SAA	Electronic	Yes

11c. Does the system receive SBU/PII from State or local agencies? No

11d. Does the system receive SBU/PII from other sources? No

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 PCLIA	Approval Date	SA&A?	Authorization Date
Account Management Services (AMS)	Yes	01/18/2018	Yes	05/08/2018

Identify the authority and for what purpose? Internal Revenue Code Sections 6001, 6011, 6012e(a), 6019. Purpose is for tax administration.

12b. Does this system disseminate SBU/PII to other Federal agencies? Yes

If **yes** identify the full names of the federal agency(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
HHS CMS SSA	Electronic	Yes

Identify the authority and for what purpose? Internal Revenue Code Sections 6001, 6011, 6012e(a), 6019. Purpose is for tax administration.

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? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

If **no**, Contact *Privacy for assistance with completing the Social Media PIA.

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

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?
Notice is provided to individuals through their contact with the source systems, such as the online health exchanges or filing of tax returns, depending on the source of the data.

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):
Individuals may decline to participate in the ACA program, but they are potentially subject to penalties, which are explained in form filing instructions and other communications provided to them by CMS.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The system will allow effected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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)

IRS 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	Yes	Read-Only

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? Access to data on the system is restricted and closely monitored. ACA management, the owners of the IRS systems, approves access via the Online 5081 system (which people use to request access to systems within the IRS). Only system administrators and developers have access to the system for performance of those duties.

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.

ISR-S provides information exchange services support between IRS and CMS, but it is not the official repository for any data or documents. Related IRS/Affordable Care Act (ACA) data retention requirements will be defined in accordance with the recordkeeping system from which the data is obtained, which is ACA Coverage Data Repository (CDR). The IRS Records Office is aware of this system's development and will be working with the system owner to draft a request for records disposition authority for submission to/approval by the National Archives. ISR-S' collection, use, retention, and disclosure of PII will be limited to what is minimally necessary for the specific purposes for which it was collected, unless specifically authorized or mandated by law. Accordingly, ISR-S follows the IRS/ACA data retention requirements.

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)? Yes

23a. If **yes**, what date was it completed? 05/10/2018

23.1 Describe in detail the system s audit trail. ISR-S will document actions initiated by users of the system and system interactions that will establish accountability, aid in investigations, and reconstruction of events. The ACA Program Level Audit Plan addresses various aspects of auditing to be performed at the program level and by the underlying common infrastructure. It describes and identifies those aspects of auditing which apply to ISR-S specifically, and how it interacts with other systems to achieve overall effective auditing for the business. Other systems include cross references to other ACA applications, the ACA General Support System (GSS), and other relevant GSS/Authorization Boundary systems such as operating systems and Database Management System (DBMS). In addition to the Security Audit Automatic Response and Auditable Events requirements, applications which process any type of or subset of taxpayer data shall capture and record the following application transactional information in audit trails: (1) employee and contractor transactions that add, delete, modify, or research a tax filer's record; (2) employee and contractor transactions that add, delete, modify, or research an employee's record (personnel and financial); (3) employee and contractor transactions that add, delete, or modify an employee's access to Employee User Portal (EUP), including changes to EUP roles or sub-roles; (4) any system transactions that alter an employee's access to the EUP, or a system's or application's role or sub role; (5) any employee or contractor transactions identified by the system owner as requiring additional oversight; and (6) any third-party transactions identified by the system owner as requiring additional oversight. Audit events that are application-specific are recorded in an audit trail log, but could also be recorded in transaction logs or error logs. Application-level audit trails monitor and log user activities. At a minimum, an event record shall specify data files opened and closed; specific actions, such as reading, editing; and deleting records or fields.

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? 10/31/2018

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?
Enterprise Consolidated Legacy Access Service (ECLAS) will undergo Developer System and Security Testing as part of the Enterprise Lifecycle (ELC) process.

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: More than 1,000,000
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