NOTE: The following reflects the information entered in the PIAMS website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: Oct 8 2014 10:21AM PIA ID Number: **1131**

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

SS8 Integrated Case Processing System, SS8ICP

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees:	Under 50,000
Number of Contractors:	Not Applicable
Members of the Public:	Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

SS8ICP is an IRS moderate risk application and resides on the Modernization & Information Technology Services (MITS)-30 General Support System (GSS). It was developed in-house in 1993. The primary purpose of the SS8ICP application is for resolution and determination regarding taxes to be withheld either by an individual or by an entity, where the individual is working. This usually arises when there is confusion regarding contractor versus employee status. In the event of discrepancies between individual and entity regarding withholding of employment and/or income taxes, the individual/entity can complete IRS Form SS-8 Determination of Worker Status for Purposes of Federal Employment Taxes and Income Tax Withholding. This form can be completed manually and mailed into the IRS, or electronically. In both cases, there are no direct feeds into the SS8ICP application. The data from Form SS-8 is manually entered into the SS8ICP application by a SS8ICP user. The data in SS8ICP is then reviewed and analyzed for determination of contractor versus employee status. In the event of contractor status, an individual is liable for Self Employment Tax (15.3%). In the event that the individual is considered an employee of the entity in question, the worker is liable for an employee's portion of Federal Insurance Contributions Act (FICA) tax (7.65%) and the firm is generally liable for employment taxes on the income under IRC section 3509, or may owe both the employer and the employee portions of FICA tax. Once a determination has been made the taxpayers receive a formal determination letter through the mail. The data stored in SS8ICP contains privacy data and includes taxpayer identification number (TIN), taxpayer name, address, contact information, and information specific to their case which could contain tax data. SS8ICP serves as an online work environment for preparing case histories, documents, reports, and responses. The system is an information and audit referral resource for field personnel. For example, in the event that an entity had not withheld the appropriate employment taxes on behalf of an individual in question, this entity could be referred to an IRS field auditor for a potential IRS audit. The SS8ICP application is not connected with any other application, and is not externally facing. The SS8ICP application shares data with one other application at the IRS called the Integrated Production Model (IPM) system, which resides on MITS-24. Each week a scheduled job runs on the SQL server (resides on the MITS-30 GSS) to pull flat file data that is on SS8ICP and transfer it to a secure IPM server via the ICP Database Server using Enterprise File Transfer Utility (EFTU). Although the SS8ICP application resides on the MITS-30 GSS, the application relies on the MITS-17 GSS for identification and authentication. Users access the data within the SS8ICP application from their workstations. SS8ICP software is installed on the workstations and the users can then traverse to the SS8ICP application from their workstations. They must have access rights in two areas. The first is within the Active Directory global user group via the MITS-17 GSS. The second area of access is to the SS8ICP database, where a manager will grant the user access to specific case files within the SS8ICP application.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 03/22/2012

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
- System is undergoing Security Assessment and Authorization Yes

6c. State any changes that have occurred to the system since the last PIA

None

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. 015-00-02-00-01-5201-00

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If **No**, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	Yes	
Employees/Personnel/HR Systems	No	
		Other Source:
Other	No	

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	Yes
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

No Other PII Records found.

10a. What is the business purpose for collecting and using the SSN ?

Documents associated with case activity containing PII and SBU data - Taxpayer employment information including data about reporting forms - Employee name and badge number - Data on returns filing from internal systems

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

IRC 6011 - requires return filingIRC 6109-1 - requires taxpayer to provide SSN to file returns26 CFR Section 301.6109-1

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

SSN reduction will be explored at the next major modification of the application. There will be no modifications until the database is moved to a new server.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

N/A. The SSN is needed to tie in all cases if taxpayer misplaces case #.

Describe the PII available in the system referred to in question 10 above.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

- Login and log-off time - Cases accessed - Case ID number - Case development documentation - Case statistics and results

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: No

If **Yes**, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: No

If **Yes**, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If **Yes**, please list the agency (or agencies) below:

d. Third party sources: Yes

If yes, the third party sources that were used are:

Other taxpayers involved in the case - Third-party contacts if warranted for case development - Internet research

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): Yes

g. Other: Yes If **Yes***, specify*: Accurint

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

The SS8ICP database is the work area and inventory management system for processing taxpayer requests for proper worker classification for the purposes of Federal employment tax purposes. In order to process the case and reach an accurate conclusion, PII data is required

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	Yes	
To provide taxpayer services	Yes	
To collect demographic data	Yes	
For employee purposes	Yes	
		If other, what is the use?
Other:	Yes	For coordination with other internal programs

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) Yes

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)	Yes	Department of Labor	Yes
State and local agency (-ies)	Yes	State employment agencies with QETP Agreements	Yes
Third party sources	No		
Other:	Yes	Other areas within IRS	

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	**AUTHORITY**
Persistent Cookies		
Web Beacons		
Session Cookies		
		If other, specify:
Other:		

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Yes

18a. If **Yes**, how is their permission granted?

Per application Subject Matter Experts, it's implied in SS8.

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

Per Subject Matter Experts, give taxpayer the right for reconsideration.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

Form Number	Form Name
Form ID: 173 Number: SS-8	Determination of Worker Status for Purposes of Federal Employment Taxes and Income Tax Withholding
Form ID: 174 Number: 1099-MISC	Miscellaneous Income
Form ID: 175 Number: W-2	Wage and Tax Statement

20b. If **No**, how was consent granted?

Written consent	
Website Opt In or Out option	
Published System of Records Notice in the Federal Register	
Other:	

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		Read Write
Managers		Read Write
System Administrators		No Access
Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

If you answered yes to contractors, please answer **22a.** *(All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)*

22a. If the contractors or contractor employees act as System Administrators or have “Root Access”, does that person hold a properly adjudicated “High Level” background investigation?

23. How is access to the PII determined and by whom?

OL5081 is used to document access requests, modifications, and terminations for all types of users. When a new user needs access to IRS systems or applications, the user's manager or designated official, access the On-Line

5081 (OL5081) application to request access for the new user. OL5081 is an online form, which includes information, such as the name of the system or application, type of access, and the manager's signature approving authorization of access. The completed OL5081 is submitted to the account administration approval group, who places the user name into the requested domain group according to the user's role. Before access is granted, the user is required to digitally sign OL5081 acknowledging his/her security responsibilities when using the system. The user signs security rules of behavior provided in the OL5081.When an existing user needs modifications to user access to IRS systems or applications, the user's manager or designated official, completes OL5081 requesting modifications to the user's access. The modification request includes information such as the name of the system or application, specific modifications requested, and the manager's signature approving modification of access. The completed OL5081 is submitted to the account administration approval group, who modifies the user's access based on the manager's request documented in the OL5081 form. Upon termination or when a user no longer needs access to the IRS systems or applications, the user's manager or designated official, completes OL5081 requesting termination of access for the user. OL5081 includes information, such as the name of the system or application and the manager's signature approving termination of access. The completed OL5081 is submitted to the account administration approval group, who terminates the user's access based on the manager's request documented on the form. Users access the data within the SS8ICP application from their workstations. SS8ICP software is installed on the workstations and the users can then traverse to the SS8ICP application from their workstations. They must have access rights in two areas. The first is within the Active Directory global user group via the MITS-17 GSS. The second area of access is to the SS8ICP database, where a manager will grant the user access to specific case files within the SS8ICP application.

---

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

The application relies on the database for the implementation of this control. User input is controlled to allow valid entries. The application requires users to provide input in the correct format for the selected field. The application limits the user to specific valid choices via lists for field completion

---

25. 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? Yes

---

25a. If **Yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

SS8ICP data associated with Form SS-8 Determination of Worker Status for Purposes of Federal Employment Taxes and Income Tax Withholding is approved for destruction after 15 years under NARA Job No. NC1-58-79-6, and published in IRS Records Control Schedule (RCS) Document 12990 under RCS 23 for Tax Administration - Examination, Item 61. However, in reviewing SS8ICP-related recordkeeping practices for completion of this PIA, system owners and the IRS Records Office determined that a re-evaluation of final disposition instructions is in order. SB/SE and the Records Office will work together to validate and potentially update dispositions for determination of worker status to better fit current data collection activities and maintenance needs, and the current electronic recordkeeping environment. The procedures for eliminating the electronic data at the end of the retention period are found in Internal Revenue Manuals (IRM) 1.15.2 Types of Records and Their Lifecycles, 1.15.3 Disposing of Records, and 1.15.6 Managing Electronic Records. Information ages off (is deleted from) the database at varying intervals, no less than 15 years.

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.

---

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
The SS8ICP system receives data from MITS-30 system which has its own controls for administrative and technical controls and therefore SS8ICP assumes that the data is secure when it is provided by MITS-30.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

Same as above: The SS8ICP system receives data from MITS-30 system which has its own controls for administrative and technical controls and therefore SS8ICP assumes that the data is secure when it is provided by MITS-30.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

Testing is conducted annually to ensure the selected controls are functioning correctly. When testing of a security control reveals that the control is not functioning as expected, the control deficiency is documented in the system's plan of action and milestones (POA&M). All test results are documented and reported to Business Unit (BU) Security Project Management Office (PMO). The security state of the application is then reported to the appropriate organizational officials annually as defined in Treasury Directives Policy (TDP) 85-01.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*? No

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORNS Number	SORNS Name
SORN ID: 82 Number: 24.030	Individual Master File (CADE)
SORN ID: 83 Number: 26.046	Business Master File
SORN ID: 84 Number: 34.037	Audit Trail and Security Records System

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No

32a. If **Yes** to any of the above, please describe:

N/A