

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: February 18, 2014

PIA ID Number: 539

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

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

FedState, Fedstate

2a. Has the name of the system changed? Yes

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

These extracts could be listed as FedState or GLDEP Extracts as follows: 1099 MISC, Appeals, BMF, BRTF, Corporate Affiliations, CP2000, Exam, FEIN, ITPI, IMF, IRTF, IRMF by Payee State Code, IRMF Non-resident, ITIN, Levy, Military Combat Zone, Non-Itemizer, PTIN, TAR. Also could be listed as NSA: 138 – 1099 and 152 – AIMS Extract.

3. Identify how many individuals the system contains information on

Number of Employees: Not Applicable

Number of Contractors: Not Applicable

Members of the Public: Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

Government mandate to share federal tax information with qualifying state agencies under the authority of IRC 6103(d) for the purposes of state tax administration. Due process is provided outside the database pursuant to 26 USC.

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: 09/13/2013

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 No
-

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

PIA 506 is being expanded to include additional FedState (GLDEP) extracts that are provided to qualifying state agencies under IRC 6103(d).

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'. 3049999999999979526, 3049999999999979011, 4049999999999979024, 4049999999999979516, 4049999999999979592, 4049999999999979675, 4049999999999979803

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
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 No *Other Source:* _____

-
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	No
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: Yes

PII Name On Public? On Employee?

IMF Yes No
BMF Yes No
IRTF Yes No
BRTF Yes No
ITIN Yes No
FEIN Yes No

-
- 10a. What is the business purpose for collecting and using the SSN ?
matching state records to federal records for the purpose of state tax administration.

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.)
The authority is under IRC 6103(d).
-

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

n/a

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

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

Extracts pull federal data from the IMF, BMF, IRTF, BRTF, ITIN, IRMF, AIMS, PTIN, and FEIN data files.

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.

The Governmental Liaison's office have an annual application process for each state wishing to participate in a federal extract. They must apply not only for the extract, but in some cases for individual fields. Signed forms are used to distinguish participating agencies. Participating agencies have extracts created. Record counts are provided for each extract. This is flat file processing and not necessarily a "system".

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: Yes

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

System Name **Current PIA?** **PIA Approval Date** **SA & A?** **Authorization Date**

IRTF	No		No	
BRTF	No		No	
ITIN	No		No	
IMF	No		No	
BMF	No		No	
FEIN	No		No	
IRMF	No		No	
AIMS	No		No	
PTIN	No		No	
IRTF	No		No	
BRTF	No		No	
ITIN	No		No	
IMF	No		No	
BMF	No		No	
FEIN	No		No	
IRMF	No		No	
AIMS	No		No	
PTIN	No		No	

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? No

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

20. Did any of the PII provided to this system originate from any IRS issued forms? No

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

No forms found.

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

Written consent No

Website Opt In or Out option No

Published System of Records Notice in the Federal Register No

Other: No

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:	<u>Yes</u>	
Users		<u>No Access</u>
Managers		<u>No Access</u>
System Administrators		<u>Read Write</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></u>

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?

Only QA and SA's have access to production data. If there is a programming issue, temporary read access may be granted to application developers for debugging purposes or for related testing purposes.

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

There is a series of business rules that get run against the production files to make sure they are as accurate and complete as possible.

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.

FedState data is approved as temporary, subject to destruction when no longer needed for operational purposes but no longer than 5 years. System data is scheduled under several NARA-approved disposition authorities: (IMF/IRTF Extracts) Job No. N1-58-09-23, published in IRS Document 12990 under Records Control Schedule (RCS) 18, item 53; (BMF Extracts) Job No. N1-58-09-22, published in IRS Document 12990 under RCS 18, item 54; and (BRTF Extracts) Job No. N1-58-09-24, published in IRS Document 12990 under RCS 18, item 55.

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.

Under general GSS for MCC mainframe.

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

at rest under GSS. Once the files are created, EFTU transfers them to a secured Drop Box. The participating state agencies can then access only their folder and then have access to only their files.

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? No

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

under general GSS for MCC mainframe.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

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.

No SORN Records found.

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:

NA