

---

**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 Submission: Mar. 20, 2012 1:03PM

PIA ID Number: 175

---

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):

**527 Political Action Committee/Political Organization Filing and Disclosure, (527 PAC/POFD)**

---

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: Not Applicable

Number of Contractors: Not Applicable

Members of the Public: Over 1,000,000

---

4. Responsible Parties:

---

N/A

---

5. General Business Purpose of System

---

527 PAC/POFD is an IRS system, managed under the Tax Exempt/Government Entities (TE/GE) Business Unit. The purpose of 527 PAC/POFD is to collect, validate and store information from IRS forms 8871, 8872, and 990 (See table below). The functionality of this system is required by law to provide Political Organizations the ability to identify their status and report contributions and expenditures. Information collected from Political Organizations is required to be made available to the general public. Forms Processed by 527 PAC/POFD 8871 Notice of Section 527 Status (Electronic Only) 8872 Report of Contributions and Expenditures (Paper and Electronic) 990 Return of Organization Exempt From Income Tax (Paper Only) This system consists of two functionalities; front-end and back-end applications. POFD is the front-end application of this system, available to the public on the IRS.GOV website (<http://www.irs.gov/charities/political/>). Political Organizations register for access to submit forms electronically (Initial Form 8871 submission does not require login). All data submitted to POFD is validated, and then sent to 527 PAC. 527 PAC is the back-end application of this system. The primary responsibilities of 527 PAC is to store a secondary copy of the electronic filings; exchange certain data with Business Master File (BMF); allow the Entity Research Group to make changes to the existing electronic filings; add, delete and reset Political Organization's login accounts, and initiate the issuance of the Letter 3406SC which allows Political Organizations to file electronic Form 8872's. 527 PAC is located at Enterprise Computer Center-Memphis and receives electronic forms from POFD. Paper forms 8872 and 990 are sent to the Entity Research Group where they are scanned and converted into Tagged Image File Format (TIFF). Western Development Center (WDC), also located in Ogden, Utah, receives the scan images, converts them to Portable Document Format (PDF) images, and transmits them to the 527 PAC application. 527 PAC provides all PDF forms along with indexing information back to POFD so that the information can be made available to the public.

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: 03/23/2009

---

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**

1.) 527 PAC Module functionality was updated with a reminder provided to the user prior to session expiration. 2.) Java Runtime Environment (JRE) was upgraded from v1.5.0\_10 to v1.6.0\_26. 3.) Oracle Database Management System (DBMS) was upgraded from v10g to 11g Release 1. (527 PAC only).

---

**7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'.** 015-45-01-14-02-2358-00

---

**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	No
Social Security Number (SSN)	No	No	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	No	No	No

**Additional Types of PII:** No

No Other PII Records found.

---

**10a. Briefly describe the PII available in the system referred to in question 10 above.**

Name and address of Contributor Name and address of Recipient of Expenditures.

**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.)**

---

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

---

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

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.

Auditing events that take place for 527 PAC are captured from Entity Research Group changes to Political Organization forms or account information. This information includes: - a listing of all files processed by the system - records of all changes made to forms submitted by Political Organizations using Oracle Forms - the User ID and password deletes and resets using Oracle Forms - a record of all image transmittals - import or export files processed by the system such as filename, number of records and processed by Date. - all changes made to member records - all changes made to schedule records - all changes made to entity records For each audit event, the 527 PAC audit trail captures the date/time, user ID, type of event, subject of event, and outcome status. Auditing events captured for POFD include user login and user logout. The audit trail captures the date/time, and user ID.

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:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA &amp; A?</u>	<u>Authorization Date</u>
Business Master File (BMF)	Yes	03/16/2010	Yes	06/04/2010
Software Development Environment Sun File Server 6 (SDESF6)	Yes	04/14/2010	Yes	06/07/2010

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: No

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

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): No

g. Other: No If Yes, specify:

### 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 purpose of 527 PAC/POFD is to collect, validate and store information from IRS forms 8871, 8872, and 990. The data items are required to meet a Congressional mandate to provide Political Organizations, identified as Section 527 Organizations, the ability to disclose their political activities by filing electronic or paper submissions of Forms 8871, 8872 and 990.

### 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	<u>Yes</u>
To provide taxpayer services	<u>No</u>

To collect demographic data No  
 For employee purposes No  
 Other: No \_\_\_\_\_ *If other, what is the use?*

---

**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)	No		
State and local agency (-ies)	No		
Third party sources	No		
Other:	Yes	Public	

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

16. Does this system host a website for purposes of interacting with the public? Yes

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

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	<u>Yes</u>	<u>Mike Silvia, Director Online Experience and Operational Management</u>
Web Beacons	<u>No</u>	<u>_____</u>
Session Cookies	<u>Yes</u>	<u>_____</u>
Other:	<u>No</u>	<u>_____</u> <i>If other, specify:</i>

---

**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? Not Applicable

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

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

19a. If Yes, how does the system ensure "due process"?

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.

<u>Form Number</u>	<u>Form Name</u>
8871	Notice of Section 527 Status
8872	Political Organization Report of Contributions and Expenditures

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 Contractor 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:

	<b>Yes/No</b>	<b>Access Level</b>
IRS Employees:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>No Access</u>
System Administrators		<u>No Access</u>
Developers		<u>Read Write</u>
Contractors:	<u>Yes</u>	
Contractor Users		<u>No Access</u>
Contractor System Administrators		<u>No Access</u>
Contractor Developers		<u>Read Write</u>
Other:	<u>No</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? No

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

527 PAC relies on the Operating System and Relational Database Management System to prescribe not only who is to have access to a specific system resource but also the type of access that is permitted. Logical access controls are implemented for software programs, data files, databases, and telecommunications access. Managers base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official function. The manager will request a user be added. They must fill out Online 5081, Information System User Registration/Change Request, to request access to the application. A user's access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities

regarding access are documented in the Information Systems Security Rules on Online 5081. Assignments of individual and group permissions adhere to the provisions as outlined in the Internal Revenue Code 6103. Before contractors can access the system, they are subject to MITS Cybersecurity procedures based on contractor risk levels, depending on their role, and background investigations, which include: Low Risk National Agency Check with Inquiries (NACI), Moderate Risk National Agency Check with Credit (NACC), or High Risk Background Investigation (BI) where applicable. Access to resources (the application/database) is based on the following access criteria, as appropriate. A. Unique User Identity (User ID). B. Roles. Access to information is controlled by the job assignment or function. C. Access Mode. Common access modes, which can be used in operating or application systems, include read, write, execute, and delete. Other specialized access modes (more often found in applications) include create or search. These criteria are used in conjunction with one another. POFD relies on MITS Cybersecurity procedures based on contractor risk levels. Contractors with access to POFD are designated IRS.GOV Technical Architecture Team members responsible for maintaining the applications and software which reside in the IRS.GOV architecture. This includes application administrators and build managers. None of the Technical Architecture group members are required to possess a security clearance for system access. The positions occupied by the IRS.GOV Technical Architecture group members are designated as ADP II (Non-critical Sensitive). The IRS.GOV Technical Architecture group members must be American citizens.

---

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

Paper Forms 8872 and 990 are reviewed for accuracy, timelines, and completeness. The forms are stamped with a date upon receipt, scanned, and transmitted to 527 PAC. 527 PAC then sends the imaged forms to POFD and they become available to the public. Electronic Forms 8871 and 8872 filed on the POFD web-site are validated against requirements/business rules established by business owner and documented in the POFD Requirements Traceability Matrix (RTM) and Design Document. Additionally, 527 PAC performs same validation of the Electronic Forms 8871/8872 on the fields that the Entity Research Group is allowed to alter whenever a subsequent change is required to be made post submission. To ensure that file transmission is not corrupted during transmission, there are control files with each exchanged listing the files, their byte count and checksum. This allows the receiving site to compare the information to ensure the integrity of the files.

---

**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.**

The IRS Records Office and TEGE are working together to evaluate and update RCS 24 to better reflect current business practices and records maintenance needs, including the movement to more electronic-based recordkeeping systems. TEGE's use of 527 PAC/POFD and other electronic systems may result in updated disposition authorities for traditional TEGE-related records series. Paper-based retentions for recordkeeping copies of IR Forms 990 and 8872 are covered under Internal Revenue Manual (IRM) 1.15.29 Records Control Schedule for Submissions Processing Campus Records, item 66. A National Archives-approved retention of IR Form 8871 has yet to be identified. Records are disposed of in accordance with prescribed IRM Records Control Schedules and Law Enforcement Manual procedures. Media protection policy and procedures are formally documented in IRM 10.8.1 and IRM 1.15.2, Types of Records and Their Life Cycle. TEGE must develop a plan to purge 527 PAC/POFD records eligible for destruction in accordance with IRS Records Management Requirements in IRMs 1.15.3 Disposing of Records and 1.15.6 Managing Electronic Records. TEGE and IRS Records Office staff will coordinate the scheduling of any system records identified as unscheduled or in need of updated disposition approvals. Prior to the disposal or transfer of a system, sensitive data and software is removed/eliminated from the memory and external storage devices.

**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.**

527 PAC/POFD - PII data is stored in the database. User password tables are stored encrypted using Oracle built-in encryption. When the user retrieves the record it is unencrypted. Logical access controls are in place to allow only authorized users to access the application and its data.

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

Application data backups performed by the supporting GSSs are encrypted using NetBackup.

**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.**

IRS Enterprise Continuous Monitoring procedures are in place for the application. These procedures are completed annually to ensure the application and its data are properly secured. In addition, the Security Assessment and Authorization (SA&A) process is completed every three years or when a significant change is made to the system.

**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)?**

**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.**

<u>SORNS Number</u>	<u>SORNS Name</u>
Treasury/IRS 50.001	Employee Plans/Exempt Organization Correspondence
Treasury/IRS 42.001	Examination Administrative File
Treasury/IRS 00.001	Correspondence Files (including Stakeholder Relati
Treasury/IRS 24.046	CADE Business Master File (BMF)
Treasury/IRS 34.037	IRS 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)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

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

Not applicable

[View other PIAs on IRS.gov](#)