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: January 30, 2015 PIA ID Number: **1235**

1. What type of system is this? 527 Political Action Committee / Political Organization Filing and Disclosure, 527 PAC-POFD

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, and milestone of the most recent PIA.

527 Political Action Committee / Political Organization Filing and Disclosure, 527 PAC-POFD

Next, enter the **date** of the most recent PIA. 4/17/2012 12:00:00 AM

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? Yes

If yes, explain what changes were made. Current PIA expires April 2015. This is a renewal of that PIA.

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
Yes	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.

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. 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), and 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). POFD MTB Linux, located in Kearneysville, West Virginia, 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

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information, 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 variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes	On Primary	No	On Spouse	No	On Dependent

If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

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

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

527 PAC-POFD application contain the EIN of political organizations that are filers. There is no planned mitigation strategy to eliminate this EIN requirement for filing and disclosure.

Question 6a requires an input on who the variation of SSN is collected on. We had no choice but to enter Primary, but it must be noted that the variation of SSN is of political organizations and not individuals.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates according to Privacy Requirements? (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
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	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
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
No	Tax Account Information	No	No	No
No	Live Tax Data	No	No	No

6c. Does this system contain SBU information the system that 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 Letter of Understanding (LOU)	Documents that have been marked OUO or LOU
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? Yes

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

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 variations) are used, explicitly explain why use of SSNs meets this criteria. 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.

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.

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 the 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.

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 50.001	Tax Exempt & Government Entities (TE/GE) Correspondence
IRS 42.001	Examination Administrative File
IRS 00.001	Correspondence Files and Control Files
IRS 24.046	Customer Account Data Engine Business Master File
IRS 34.037	IRS Audit Trail and Security Records System

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

N/A

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 PIA?	PIA Approval Date	SA & A?	Authorization Date
Business Master File	Yes	06/02/2014	Yes	05/23/2013

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? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
SS-4	Application for Employer Identification Number
8453X	Political Organization Declaration for Electronic Filing of Notice of Section 527 Status
8871	Political Organization Notice of Section 527 Status
8872	Political Organization Report of Contributions and Expenditures
990	Return of Organization Exempt from Income Tax
990EZ	Short Form Return of Organization Exempt from Income Tax

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
Generalized Master File (GMF)	No		No	
Automated Print (IAP)	No		No	

Identify the authority and for what purpose? Per Internal Revenue Code sections 6001, 6011, 6012(a), and IRC 26–USC 527(K), 527 PAC passes POFD filing information to the

GMF, and sends generated credentials to the IAP which allows filers to continue filing to the POFD website.

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? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, cloud, 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? Yes

16a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

If **yes**, what was the approved level of authentication?

Level 1: Little or no confidence in the asserted identity's validity.

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?
Applicants must access the IRS.gov website to enter the POFD application. The website explains the information that will be capture during the application process.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

If no, why not? N/A Information is collected from Forms filed by the taxpayer with the Internal Revenue Service.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The system will allow affected parties the opportunity to clarify or dispute negative determinations per the examination appeals process as outlined in IRS Publication 1 - Your Rights as a Taxpayer,

and IRS Publication 5 - Your Appeal Rights and How To Prepare a Protest If You Don't Agree. 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 Contractor 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	Yes	Read and Write
Managers	No	
Sys. Administrators	Yes	Read and Write
Developers	No	

Contractor Employees? Yes

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

21a. How is access to SBU/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.

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? Yes

22a. 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, 8871 and 8872 are covered under Records Control Schedule (RCS) 29 for Submissions Processing Campus Records, item 66 (published in Document 12990). 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.

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? 6/22/2012 12:00:00 AM

23.1 Describe in detail the system s audit trail. 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 lockout. The audit trail captures the date/time, and user ID.

I.2 SA&A OR ECM-R

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. A System Test plan has never been completed.

K. LIVE DATA TESTING

25. Does this system use, or plan to use Live 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: Not Applicable
26d. Other: Yes

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).
Political Organizations

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 or IRS contractors 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