

## **Section 527 Political Action Committee/Political Organization Filing and Disclosure (527 PAC/POFD) – Privacy Impact Assessment (PIA)**

**PIA Approval Date: Mar. 23, 2009**

### **System Overview**

The Section 527 Political Action Committee (527 PAC) in conjunction with Political Organization and Filing Disclosure (POFD) is an Internal Revenue Service (IRS) application controlled under the IRS TEGE Business Unit. The purpose of the 527 PAC/POFD system is to collect, validate, and store information from IRS Forms 8871 and 8872 which are collected from political organizations through a web site hosted and maintained by contractor support.

The functionality of this application 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.

### **Systems of Records Notice (SORN):**

- IRS 50.001 Employee Plans/Exempt Organization Correspondence Control Records
- IRS 42.001 Examination Administrative File
- IRS 00.001 Correspondence Files (including Stakeholder Relationship Files) Correspondence Control Files
- IRS 24.046 CADE Business Master File (BMF)
- IRS 34.037 IRS Audit Trail and Security Records System

### **Data in the System**

#### **1. Describe the information (data elements and fields) available in the system in the following categories:**

- A. Taxpayer – Data from Forms 8871, 8872, and 990 on organization taxpayers (publicly available):

##### **Header data for all Forms:**

- Organization name
- Employer Identification Number (EIN)
- Organization address
- Organization e-mail (F8871& 8872)
- Organization representative contact and address (F8871& 8872)
- Organization custodian of records and address (F8871& 8872)
- Date organization formed ( F8872)
- Date established ( F8871)
- Date of material change ( F8871)
- Election Authority (F 8871)
- Election Authority Identification Number (F8871)
- Name and address of principal officer (F990)
- Website (F990)
- Telephone number ( F990)

##### **Form 8871:**

- Names of highly compensated organization officers, title, and address

- Document Locator Number
- Tax Period,
- Filing Reporting Type (Initial, Amended, Final),
- Received Date
- Exemption from filing F8872 Code
- Exemption from filing F990 Code

**Form 8872 (including Schedules A and B):**

- Report type (e.g., quarter, annual)
- Total amount of reported contributions
- Total amount of reported expenditures
- Contributors' names, mailing addresses, and zip codes
- Contributors' employers, occupations, and aggregate annual contributions
- Amount of contributions
- Recipients' names, mailing addresses, and zip codes
- Recipients' employers, occupations, and aggregate annual contributions
- Amount of contributions
- DLN
- Tax Period
- Filing Reporting Type (Initial, Amended, Final, Change)
- Received date
- Report Type (1st/2nd/3rd Quarters, Monthly, Mid Year, Pre/Post Election and End of Year)
- Total Contribution

**Total Expenditure- Form 990 (including Schedule B):**

- Organization type (e.g., 527)
- Organization gross receipts and revenue
- Organization Expenditures
- Organization Balance Sheet data
- Names of organization officers, title, and address
- Contributors' names, mailing addresses, and zip codes
- Contributors' employers, occupations, and aggregate annual contributions
- Amount of contributions
- DLN
- Tax Period
- Received Date

**Web Access credentials to fill out F8872:**

- Taxpayer User ID and Password (required to file Forms 8871 and 8872 electronically after the initial Form 8871 is filed):
- Organization User Identification (ID)
- Organization Password

B. Employee – The 527 PAC/POFD system does not capture information about an IRS employee. The electronic version of the Form 8871/8872 data is stored internally on a database and the data is made available to IRS employees who have been given privileges to view and update parts of the data. When a change is made to the database, information about the change and the user who made the change is recorded on an audit trail.

- C. Audit Trail Information – 527 PAC maintains an audit table to effectively trace user actions within the system. Audit trails will include sufficient information to establish what events occurred and who (or what) caused them. For each recorded event, the audit record (event record) shall identify:
- Date and time when the event occurred
  - Employee Database Identifier associated with the event
  - Copy of previous record before change

**2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.**

- A. IRS – Four Business Master File (BMF) output files from Run 12044 are generated and sent to 527 PAC on a weekly basis. The information consists of mailing addresses for each political organization. It is used to ensure that the user identification and password, generated by 527 PAC, are sent to the proper destination. BMF output files are also used to identify those Political Organizations that have filed the required Form 8871 and signed Form 8453X and therefore are eligible to receive the Letter 3406SC with the credentials to log into the POFD website.
- B. Taxpayer – Paper versions of the Forms 8872, 990 and attachments, submitted by political organizations are scanned into Adobe PDF format and transferred to 527 PAC. The file naming convention consists of the organization EIN, Form Name and Occurrence. The following information is obtained from the taxpayer:

Data from Forms 8871, 8872, and 990 on organization taxpayers (publicly available)  
Header data for all Forms: (please refer to form data fields listed in question #1).

- C. Other Third Party Sources – Data from the Forms 8871 and 8872 that is entered by the political organization using the POFD website is captured and transferred via Secure FTP (File Transfer Protocol) from POFD to 527 PAC. The information is sent through a secured Virtual Private Network (VPN). There is no other Third Party Source that provides data for the 527PAC/POFD system. FTP or SFTP is only the communication method by which 527PAC and POFD communicate. No third parties are supplying additional information not already reported sections A or B of the question.

**3. Is each data item required for the business purpose of the system? Explain.**

Yes. 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.

**4. How will each data item 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 527PAC. PAC527 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, 527PAC 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.

**5. Is there another source for the data? Explain how that source is or is not used.**

No, there is no other source of the data available to the public.

**6. Generally, how will data be retrieved by the user?**

Entity Research Group personnel within the Campus have the ability to access the electronic Forms 8871 and 8872. They also can access the paper Forms 8871, 8872 and 990 via an internal web site using a browser. These users can retrieve the data by EIN or Name of Organization. Filers have the ability to access the POFD web-site to electronically file initial, amended, and/or final Forms 8871 and 8872. Electronically filing requires a User ID and Password. The IRS issues a User ID and Password to filers once the initial Form 8871 is electronically filed and IRS receives the filers' paper Form 8453X. The general public has view only access of the Forms 8871, 8872 and 990 via the Internet. View only access does not require User IDs or passwords.

**7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?**

Yes. PAC 527 data is retrievable by EIN or organization name. However, PAC527 data is not retrievable or viewable by the taxpayer or the general public. POFD viewers can retrieve data by any field on the Forms 8871 or 8872. The personal information available on those forms is required to be disclosed to the general public by statute.

**Access to the Data**

**8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?**

527PAC is maintained by IRS personnel which include the following roles:

- System Administrators (SA's) have the ability to install, upgrade, and maintain software, operating systems, and applications. SA's also monitor the change control process, system security controls, and grant system access.
- Database Administrators (DBA's) create and update database tables and indexes.
- Application Users are responsible for the daily operations of the hardware, operating systems, installed applications, and the proper use of the security features.

POFD sits on the IRS.GOV web-site and is maintained by a non-governmental third-party contractor. The contractor maintains roles similar to those of the IRS and has the ability to install, upgrade, and maintain software, operating systems, and applications. They monitor the change control process, system security controls, and grant system access. They also create and update database tables and indexes. While they have access to the POFD application, they do not have access to the 527PAC application. Additionally, contractors do not have access to the forms submitted by the organizational filer.

External:

- Organization Filers: Organizational filers have the rights to add, change, or delete only their specific organization's forms based on their user ID and password.
- General public (web accessible output from Forms 8871, 8872, and 990 are viewable)

**9. How is access to the data by a user determined and by whom?**

527PAC 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 (NACI), Moderate Risk (NACC), or High Risk (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 database administrators, 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.

**10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared. If NO, continue to Question 12.**

Yes. Electronic 8871 and 8872 forms are identified and collected from POFD. A file is created by 527 PAC and sent for processing through General Mainline Framework (GMF) and posting to the BMF. The data shared includes:

**Form 8871:**

- DLN,
- EIN,
- Tax Period,
- Filing Reporting Type (Initial, Amended, Final),
- Received Date,
- Street Address Line 1, Street Address Line 2,
- City, State, Zip Code,
- Exemption from filing F8872 Code
- Exemption from filing F990 Code

**Form 8872:**

- DLN,
- EIN,
- Tax Period,
- Filing Reporting Type, (Initial, Amended, Final, Change),
- Received Date,
- Street Address Line 1, Street Address Line 2
- City, State, Zip Code,
- Report Type (1st/2nd/3rd Quarters, Monthly, Mid Year, Pre/Post Election and End of Year)
- Total Contribution,
- Total Expenditure

The paper 8872 and 990 forms are received by the Campus and scanned into an Adobe PDF format. These images are transferred to 527 PAC and then sent to POFD.

On a weekly basis, a userID and password file is created of initial Form 8871 filers and is ftp-ed and incorporated into a notice facsimile (the automatic printing process of the Letter 3406SC), routed to the printers at the Campus and mailed to the political organizations. The Letter 3406SC is automatically generated once 8871 and 8453X is received by IRS. User IDs/Passwords are IRS generated and are unique to the taxpayer. The taxpayer must use the User ID/password supplied by the IRS. If it is lost/forgotten the IRS will reissue a new User ID/password. The access credentials are also sent to POFD so that political organizations can log into the website and report their contributions using Form 8872.

Business Master File (BMF)

**11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?**

Yes. The following system holds a current Certification and Accreditation in the MITS Cybersecurity Master Inventory:

**BMF**

- C&A received on 6/17/2007, expires on 6/14/2010
- Privacy Impact Assessment (PIA) received on 8/10/2007, expires on 8/10/2010

**12. Will other agencies provide, receive, or share data in any form with this system?**

No. Other agencies will not provide, receive, or share data in any form with the 527 PAC/POFD system.

**Administrative Controls of Data****13. What are the procedures for eliminating the data at the end of the retention period?**

Prior to the disposal or transfer of a system, sensitive data and software is removed/eliminated from the memory and external storage devices. Records are disposed of in accordance with prescribed Internal Revenue Manual (IRM) and Law Enforcement Manual procedures. Media protection policy and procedures are formally documented in IRM 10.8.1 and IRM 1.15.2, Records Management.

Hard copy media that is no longer required or needed is disposed of (e.g., shredded, burned) in accordance with IRM 1.15.24, Records Control Schedule for Tax-Exempt and Governmental Entities.

Data sets that are no longer required or needed are destroyed or eliminated in accordance with IRM 1.15.6, Managing Electronic Records.

**14. Will this system use technology in a new way?**

No. The 527 PAC/POFD system will not use technology in a new way.

**15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.**

Yes (for groups). The business purpose of the system is to provide a repository for the Forms 8871, 8872 and 990 information filed by political organizations and is used for research purposes.

**16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.**

Yes (for groups). The system provides the capability to monitor filings of political organizations to support the business purpose of the system. The Functional Security Coordinator and System Administrators monitor the history files for any unauthorized actions on the part of a 527 PAC User.

**17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?**

No. All taxpayers will be treated equally. All Forms 8871, 8872, and 990 data, whether sent in by paper or electronic form, are processed and stored using the same automated method and all information is made available for public viewing via the POFD website.

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

No. The system does not make determinations. All Forms 8871, 8872 and 990 data, whether sent in by paper or electronic form, are processed and stored using the same automated method and all information is made available for public viewing via the POFD website.

**19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?**

No. 527 PAC does not use persistent cookies. POFD is a web-based system but does not use persistent cookies or other tracking devices. However, when a political organization files electronically via POFD, they are identified by their login upon accessing the system. POFD also uses a tool called web-trend to gauge the number of web pages that have been viewed.

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