

Date of Approval: 05/07/2026
Questionnaire Number: 2847

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

527 Political Action Committee Political Organization Filing and Disclosure
Website

Acronym:

527PAC/POFD

Business Unit

Tax Exempt and Government Entities

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

527 Political Action Committee Political Organization Filing and Disclosure Website (527PAC/POFD) is an IRS system, managed under the Tax Exempt/Government Entities (TE/GE) Business Unit. The purpose of 527PAC/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 with the ability to identify their status and report contributions and expenditures. Information collected from Political Organizations is required to be made available to the public. 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-&-Non-Profits/Political-Organizations/Political-Organization-Filing-and-Disclosure>). 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 PAC. PAC is the back-end application of this system. The primary responsibilities of 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 Organizations login accounts, and initiate the issuance of the Letter 3406SC which allows Political Organizations to file electronic Form 8872. PAC 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), receives the scan images, converts them to Portable Document Format (PDF) images, and transmits them to the PAC application. PAC provides all PDF forms along with indexing information back to POFD so that the information can be made available to the public.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

PAC and POFD transmit data using Secure File Transfer Protocol (SFTP). The data transfer uses the current Virtual Private Network (VPN) and Port 22 on the POFD FTP server. Forms 8871/8872/990 images and indexes are transferred from PAC to POFD. Logins are transferred from PAC to POFD. This is used by Political Organizations to log into POFD front-end application to file amended/final electronic 8871/8872. Corrections to electronic 8871/8872 are transferred from PAC to POFD. Form 8871 can be abbreviated or the full version. New electronic 8871/8872 submissions are picked up from POFD and transferred over to PAC by the PAC application. Miscellaneous control files are exchanged between systems to verify Checksums of files after transfers. The only data that is exchanged that is not available to the public via the Search POFD routine is the login information.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address

Email Address

Employer Identification Number

Federal Tax Information (FTI)

Internet Protocol Address (IP Address)

Name
Other
Standard Employee Identifier (SEID)

Please explain the other type(s) of PII that this project uses.

Device ID

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

PII for personnel administration - 5 USC

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?

No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

System

3 What Tier designation has been applied to your system? (Number)

2

4 Is this a new system?

No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?

Yes

4.11 What is the previous PCLIA number?

2536

4.12 What is the previous PCLIA title (system name)?

527 Political Action Committee Political Organization Filing and Disclosure

Website

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

Updating the PCLIA in response to the recent FISMA-26 annual security testing where the following deficiency was identified: 527 PAC/POFD does not comply with privacy impact assessment requirements to ensure an accurate PCLIA was completed, and appropriate privacy protections are considered. 527 PAC/POFD has an approved PCLIA 2536 that identifies and mitigates privacy risks created by

the system. However, the PCLIA incorrectly identifies Social Security numbers (SSNs) as personally identifiable information (PII) collected by the system. The PCLIA is being corrected to remove the collection of social security numbers.

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Tax Exempt & Government Entities (TE/GE) Investment Executive Steering Committee (IESC)

9 Is this System listed on As-Built-Architecture (ABA)? If the system is not in the ABA, then contact the ABA (<https://ea.web.irs.gov/aba/index.html>) for assistance.

Yes

9.1 What is the ABA ID?

210006

9.2 If there are other applications covered by this PCLIA, then list their ABA IDs separated by a comma (example: 123456,789012). If there are no other applications covered by this PCLIA, then answer N/A.

210859

10 Does this system disclose any PII to any third party outside the IRS?

Yes

10.1 Does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act?

Yes

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

No

13 Does this system/application interact with the public?

Yes

13.1 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

Yes

13.11 Please upload the approved DIRA report using the Attachments button. Select "Yes" to indicate that you have or will upload the signed DIRA form.

Yes

13.2 If individuals do not have the opportunity to give consent to collect their information for a particular use, why not?

Applicants must access the IRS.gov website to submit the POFD application. Notice, consent and due process are provided in the application instructions filed by the taxpayer, and pursuant to 5 United State Code (USC).

13.3 If the individual was not notified of the following items prior to the collection of information, why not? 1) Authority to collect the information 2) If the collection is mandatory or voluntary 3) The purpose for which their information will be used 4) Who the information will be shared with 5) The effects, if any, if they don't provide the requested information.

Applicants must access the IRS.gov website to submit the POFD application. Notice, consent and due process are provided in the application instructions filed by the taxpayer, and pursuant to 5 United State Code (USC).

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

Notice, consent and due process are provided in the application instructions filed by the taxpayer, and pursuant to 5 United State Code (USC).

15 Is this system owned and/or operated by a contractor?

Yes

15.1 If a contractor owns or operates the system, does the contractor use subcontractors; or do you require multiple contractors to operate, test, and/or maintain this system?

Yes

15.2 What PII/SBU data does the subcontractor(s) have access to?

Address, Email Address, Employer Identification Number, Federal Tax Information (FTI), Internet Protocol Address (IP Address), Name, Other, Standard Employee Identifier (SEID), Device ID

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

IRS Employees: Users - Read and Write, Managers - Read and Write, System Administrators - Read and Write, Developers - No Access
Contractor Users - NO ACCESS Contractor Managers - NO ACCESS Contractor Sys Admin - READ and WRITE ACCESS - Background Investigation completed
Contractor Developers - READ AND WRITE ACCESS - Background Investigation completed

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

527 PAC: THIS US GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!! Use of this system constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities. There is no right to privacy in this system. Unauthorized use of this system is prohibited and subject to criminal and civil penalties. POFD: This U.S. Government system is for authorized use only! Use is consent to authorized monitoring, capturing, etc. & no rights to privacy.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

50,000 to 100,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

More than 1,000,000

22 How is access to SBU/PII determined and by whom?

For PAC, the approximate number of internal users varies between two and five. For POFD, the number of external users is in the thousands. The table below identifies the component, interface, authentication type, user group, organization, and whether the interface is external or internal to the IRS. There are five types of users with access to PAC/POFD: - PAC Developers. The developer manages application code changes, performs maintenance, and processes form transmittals for PAC. The developers have access to DEV only when performing these functions. - POFD Developers. The developer manages application code changes,

performs maintenance, and processes form transmittals for POFD. The developers have access to DEV only when performing these functions. - PAC Entity Research Group is responsible for the creation and management of Political Organization accounts and can make updates/changes to submitted forms. All PAC users have access to the application through the local IRS LAN or WAN. - POFD Filers. POFD filers are organizations who utilize the application to submit and update Forms 8871 and 8872. - POFD General Public. The public has view only to access forms. IRS utilizes the BEARS process to streamline the request process for adding authorized IRS employees, vendors, and contractors, as users on IRS computer systems and applications. Users access the BEARS application via a web site on the IRS Intranet. The user enters their Standard Employee Identifier (SEID), which is crosschecked against identity data received from the authoritative source, HR Connect, via the IRS PDS Hub (Web Service). Approval for access to an IRS application is a multi-step process. Once the request has been approved, the user is notified via an e-mail of their logon ID and initial password, if any.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

24 Explain any privacy and civil liberties risks related to privacy controls.

Updating the PCLIA in response to the recent FISMA-26 annual security testing where the following deficiency was identified: 527 PAC/POFD does not comply with privacy impact assessment requirements to ensure an accurate PCLIA was completed, and appropriate privacy protections are considered. 527 PAC/POFD has an approved PCLIA 2536 that identifies and mitigates privacy risks created by the system. However, the PCLIA incorrectly identifies Social Security numbers (SSNs) as personally identifiable information (PII) collected by the system.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

Yes

26 Describe this system's audit trail in detail. Provide supporting documents.

Auditable events are documented in the Internal Revenue Manual (IRM) 10.8.1. The IRM states that all IRS information systems capture and record the auditable events listed in the IRM based on their FIPS PUB 199 overall system security categorization. The application audits events as required by the IRM and automatically sends the log files to Security Audit and Analysis System (SAAS) daily. The audit trail will contain the audit trail elements as required in current IRM 10.8.3, Audit Logging Security Standards.

27 Does this system use or plan to use SBU data in a non-production environment?

No

Interfaces

Interface Type

IRS or Treasury Contractor

Agency Name

Print Automation (PRINT)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Electronic File Transfer Utility (EFTU)

Interface Type

IRS Systems, file, or database

Agency Name

Generalized Master File (GMF)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Electronic File Transfer Utility (EFTU)

Interface Type

IRS Systems, file, or database

Agency Name

Political Organization Filing & Disclosure (POFD)

Incoming/Outgoing

Both

Transfer Method

Secure File Transfer Protocol (SFTP)

Interface Type

IRS Systems, file, or database

Agency Name

Business Master File

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Electronic File Transfer Utility (EFTU)

Interface Type

IRS Systems, file, or database

Agency Name

Statistics of Income Distributed Processing System (SOI DPS)

Incoming/Outgoing

Incoming (Receiving)

Transfer Method
Secure File Transfer Protocol (SFTP)

Interface Type
IRS Systems, file, or database

Agency Name
SPLUNK

Incoming/Outgoing
Outgoing (Sending)

Transfer Method
Secure File Transfer Protocol (SFTP)

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 24.046 - Customer Account Data Engine Business Master File
Describe the IRS use and relevance of this SORN.
The PAC/POFD system maintain records of Form 8871/8872 and 990 filings and sends transactions of filing to the Business Master File.

SORN Number & Name

IRS 42.001 - Examination Administrative Files
Describe the IRS use and relevance of this SORN.
To document the examinations of tax returns or other determinations as to a taxpayer's tax liability; to document determinations whether or not to examine a taxpayer; and to analyze trends in taxpayer compliance.

SORN Number & Name

IRS 00.001 - Correspondence Files and Correspondence Control Files
Describe the IRS use and relevance of this SORN.
Correspondence concerning political filings & Letter 3406SC is received and sent with respect to matters under the jurisdiction of the IRS. Correspondence includes letters, telegrams, memoranda of telephone calls, email, and other forms of communication. Correspondence may be included in other systems of records described by specific notices.

SORN Number & Name

IRS 50.001 - Tax Exempt & Government Entities (TE/GE)
Correspondence Control Records

Describe the IRS use and relevance of this SORN.

Requesters of letter rulings and determination letters, and subjects of field office requests for technical advice and assistance and other correspondence, including correspondence associated with section 527 organizations.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

Records concerning the use of IRS computing equipment or other resources by employees, contractors, or other individuals to access IRS information; records concerning individuals whose information was accessed using IRS computing equipment/resources; records identifying what information was accessed; records concerned the use of IRS computer equipment and other resources to send electronic communications.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

Information Systems Security Records

What is the GRS/RCS Item Number?

GRS 3.2 Item 30

What type of Records is this for?

Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.

System access records. These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.

Records are used to monitor inappropriate systems access by users.

Includes records such as: user profiles log-in files password files audit trail files and extracts system usage files cost-back files used to assess charges for system use.

Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. Exclusion 1. Excludes records relating to electronic signatures. Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. Exclusion 1. Excludes records relating to electronic signatures. Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. Exclusion 1. Excludes records relating to electronic signatures. Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. Exclusion 1. Excludes records relating to electronic signatures. Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

What is the disposition schedule?

Destroy when business use ceases.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

Information Systems Security Records

What is the GRS/RCS Item Number?

GRS 3.2 Item 31

What type of Records is this for?

Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.

System access records. These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: user profiles, log-in files, password files, audit trail files and extracts, system usage files, cost-back files used to assess charges for system use. Systems requiring special accountability for access. These are user identification records associated with systems which are highly sensitive and potentially vulnerable. Exclusion 1. Excludes records relating to electronic signatures. Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

What is the disposition schedule?

Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Tax Administration - Tax Exempt and Government Entities (TE/GE)

What is the GRS/RCS Item Number?

RCS 24 Item 84

What type of Records is this for?

Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.

527 Political Action Committee/Political Organization Filing and Disclosure (527PAC/POFD) System and Records. The 527 Political Action Committee (PAC)/Political Organization Filing & Disclosure (POFD) System collects, validates, stores, and discloses information from IRS Forms 8871, 8872, and 990 filed by political action committees. This system is required by law to provide political organizations with the ability to identify their status and report contributions and expenditures. Information collected from political organizations is required to be made available to the public. The 527PAC/POFD application consists of two separate

systems: The POFD (public facing) web application captures electronically submitted Forms 8871 (Political Organization Notice of Section 527 Status) and Forms 8872 (Political Organization Report of Contributions and Expenditures) from political organizations on a real-time basis. POFD sends copies of the input to the PAC (Disclosure site).

What is the disposition schedule?

(A) 1. Delete/Destroy electronic data after verification of successful ingest/incorporation into system master file. 2. Delete/Destroy after verification of successful ingest/incorporation into system master file. (B) 1. Cut off at end of calendar year in which application is received. Delete/Destroy 200 years after cutoff. 2. Cut off at end of calendar year in which application is received. Delete/Destroy seven (7) years after cutoff. 3. Cut off at end of calendar year in which application is received. Delete/Destroy seven (7) years after cutoff. (C) Delete/Destroy when no longer needed for administrative, legal, audit, or other operational purposes, whichever is later.

Data Locations

What type of site is this?

System

What is the name of the System?

SPLUNK

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the System.

SPLUNK implements a data warehousing solution that provides on-line analytical processing (OLAP) access to audit trail data to detect security violations. SPLUNK enables users to analyze and report on audit log data for both Modernized and Current Processing Environment (CPE) applications.

What are the incoming connections to this System?

None

What are the outgoing connections from this System?

Audit data and modernized application audit trails are transmitted directly to SPLUNK in Extensible Markup Language (XML) format via EFTU daily. SPLUNK collects, stores, and reports audit trail data for the investigation of instances of Unauthorized Access (UNAX) violations against Internal Revenue Service (IRS) applications.