Online Payment Agreement (OPA) – Privacy Impact Assessment

PIA Approval Date – Apr. 7, 2010

System Overview:

Online Payment Agreement (OPA) is an Integrated Customer Communications Environment (ICCE) Web Applications (Web Apps) applet that has been updated to include additional functionality for the 2009 filing season. The applet was developed in response to an increase in the number of requests for Online Payment Agreements and the limited number of resources available. Requesting and complying with a payment agreement generates questions and contacts – by phone, mail and walk in – but they don't always require human interaction. Taxpayers must be offered a way to request a Payment Agreement (PA) and comply with its terms – quickly, privately, and inexpensively during system hours of operation. OPA was designed to alleviate issues with the old payment agreement process and provide taxpayers with a real–time web–based application.

Systems of Records Notice (SORN):

- IRS 26.019--Taxpayer Delinquent Account Files
- 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 – The taxpayer information includes the following:
      - Taxpayer Identification Number (TIN)
      - Social Security Number (SSN). The SSN is required for authentication and is required to provide the services requested by the taxpayer. There is no possible replacement for the SSN.
      - Individual Taxpayer Identification Number (ITIN), used for non–US citizens that work and pay taxes in the US
      - Personal Identification Number (PIN)
      - Caller Identification (CID), from balance due notice
      - Date of Birth (DOB)
      - Bank Name
      - Bank Address
      - Bank Account Name(s) (primary, joint, etc.)
      - Type of Account
      - Account Address
      - Account Number
      - Routing Number
      - Employer Name
      - Employer Address
      - Employee Name (primary or secondary)
      - Address of record
      - Optional phone numbers
      - Proposed payment amount
      - Payment month or date
      - Payment option (pay now, extension or installment agreement)
      - Adjusted Gross Income (AGI) from prior year tax return

Any joint filing statues may be requested to provide the spouses TIN and DOB depending on who is listed as primary on the return and in the IRS legacy databases. Not all data elements will be requested from the taxpayer, depending on the method of payment chosen by the taxpayer. Each data element requested by the OPA application is required to provide the functionality requested by the taxpayer.

B. Audit Trail Information – OPA will collect Management Information System (MIS) data related to the taxpayer's use of the application (e.g., how many hits encountered, how many taxpayers' successfully submitted an installment agreement and what links were followed). In addition to MIS, in the current production environment, OPA sends all of its business layer outbound responses to Security Audit and Analysis System (SAAS) through Application Messaging and Data Access Service (AMDAS) on the outbound queue. AMDAS provides a secure communication service between modernized components.

C. Other – Tax preparers and others can be authorized to act on the taxpayer's behalf when the taxpayer files a Form 2848, Power of Attorney and Declaration of Representatives (PoA). PoA users can access OPA by providing his/her Centralized Authorization File (CAF) number, the taxpayer's SSN/ITIN and the taxpayer's Caller ID from the taxpayer's balance due notice. Alternatively, the PoA can provide the Signature Date of the Form 2848 (PoA) instead of the taxpayer's Caller ID.

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

A. IRS – IRS data elements associated with the taxpayer's case are obtained through access to legacy databases: Integrated Data Retrieval System (IDRS) and Corporate Files Online (CFOL) which contains:
   - Taxpayer Information File (TIF)
   - Taxpayer data provided by taxpayers via their tax returns
   - Information collected from employees who are authorized to log on to work and process requests such as audits, payment and collection activities
   - Data is retrieved through IDRS/CFOL using command codes (including TIN, PIN, CID, DOB, Address of Record, entity and module data)

B. Taxpayer – The personally identifiable information (PII) that taxpayers may submit on–line in order to fulfil their payment obligation to the IRS is referenced in question 1A of this PIA, and includes:
   - Taxpayer Identification Number (TIN)
   - Social Security Number (SSN)
   - Individual Taxpayer Identification Number (ITIN), used for non–US citizens that work and pay taxes in the US
   - Personal Identification Number (PIN)
   - Caller Identification (CID), from balance due notice
   - Date of Birth (DOB)
   - Bank Name
   - Bank Address
   - Bank Account Name(s) (primary, joint, etc.)
   - Type of Account
   - Account Address

- Account Number
- Routing Number
- Employer Name
- Employer Address
- Employee Name (primary or secondary)
- Address of record
- Optional phone numbers
- Proposed payment amount
- Payment month or date
- Payment option (pay now, extension or installment agreement)
- Adjusted Gross Income (AGI) from prior year tax return

Any joint filing statues may be requested to provide the spouses TIN and DOB depending on who is listed as primary on the return and in the IRS legacy databases.

3. Is each data item required for the business purpose of the system? Explain.
Yes. All data items collected are for the specific business purpose of providing taxpayers that owe money to the IRS the capability of setting up an installment plan via the web interface offered through OPA.

4. How will each data item be verified for accuracy, timeliness, and completeness?
OPA restricts user input through the use of multiple mechanisms. The OPA applet restricts user input through the use of a script that notifies the user if sections of the form were left blank or the input was a different type than what is acceptable for the field. OPA also pre–populates dropdown boxes (Month, Day, Year, State) for certain forms where user input is required. This adds control to the values that can be stored or processed by the system. Radio buttons or checkboxes are also used to collect user responses for application defined answers. The system also notifies the taxpayer through the use of "on screen" text examples of input restrictions. OPA also performs validations on end user input of their PIN through the authentication process.

5. Is there another source for the data? Explain how that source is or is not used.
No. OPA does not receive data from any other sources.

6. Generally, how will data be retrieved by the user?
Users of OPA may obtain the link to OPA from IRS.gov and can bookmark the site. Users are required to enter some combination of shared secrets in response to questions to verify their identity. Once they enter shared secrets and their data matches up with the IDRS/CFOL information to ensure that the information is correct, they are eligible to use the system. This is termed successful authentication. Below are the different groups of users and what shared secrets they must enter to gain access and retrieve data from the system.

- Taxpayers without a PIN must provide their TIN, CID (a Caller ID on the Balance Due notice mailed to taxpayers), and DOB
- Taxpayers with a PIN must provide their TIN and PIN
- PoA users can access OPA by providing his/her Centralized Authorization File (CAF) number, the taxpayer's SSN/ITIN and the taxpayer's Caller ID from the taxpayer's balance due notice. Alternatively, the PoA can provide the Signature Date of the Form 2848 (PoA) instead of the taxpayer's Caller ID.
- Pre–Assessed Taxpayers must provide their TIN, AGI from prior year return and DOB.
- A PoA representing a Pre–Assessed Taxpayer must provide the taxpayer's TIN, AGI and CAF number.

Any joint filing statues may be requested to provide the spouses TIN and DOB depending on who is listed as primary on the return and in the IRS legacy databases.
Data will be retrieved from IRS records by the user through the publicly available web front–end portion of the application using an encryption capable web browser such as Internet Explorer. Users will have no direct access to IRS systems beyond the front–end web server. Users will only have such access to the web server as is necessary to provide OPA with information to perform its intended purpose and view the resulting information display.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. All users of OPA are required to authenticate prior to being granted access to the applet. No access to the OPA applet is allowed without first authenticating.
Below are the different groups of users and what shared secrets they must enter to gain access and retrieve data from the system.

- Taxpayers without a PIN must provide their TIN, CID (a Caller ID on the Balance Due notice mailed to taxpayers), and DOB
- Taxpayers with a PIN must provide their TIN and PIN
- PoA users can access OPA by providing his/her Centralized Authorization File (CAF) number, the taxpayer's SSN/ITIN and the taxpayer's Caller ID from the taxpayer's balance due notice. Alternatively, the PoA can provide the Signature Date of the Form 2848 (PoA) instead of the taxpayer's Caller ID.
- Pre–Assessed Taxpayers must provide their TIN, AGI from prior year return and DOB.
- A PoA representing a Pre–Assessed Taxpayer must provide the taxpayer's TIN, AGI and CAF number.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Only Tier–2 System Administrators (SAs) have read–only access to the production database that holds the taxpayer entered data. This data is stored temporarily in the database only if the taxpayer chooses to save his or her progress within OPA before completing the payment agreement. The taxpayer may then access his or her saved data and finish the online payment agreement at a later date and time. An automatic data removal process occurs every two weeks, so taxpayers may not save information for longer than the two week duration. Taxpayers have read, write, and edit access to the front–end web server for his or her own tax information. If the taxpayer does not save his/her progress in the system, the data is removed from the OPA web–based application when the session times out. There is no other persistent data in OPA.

Note: Currently, OPA has a contractor that holds the role as the Development Database Administrator. The Development Database administrator has no access to the Production database.

9. How is access to the data by a user determined and by whom?
Access to the data by taxpayers is determined by the taxpayer entering valid shared secrets. Please refer to question 6 above to review the shared secrets needed for authentication. The development Database Administrator Contractor has a valid National Agency Check and Inquiries (Coverage 2) for a Moderate risk contractor position as required by IRM 1.23.2.2. that is obtained by the Department of Treasury prior to being granted access to development IRS systems. They do not have access to

production systems and databases. The Production Database Administrators (DBA's) DBAs and System Administrators (SA's) gain access through manager approval and the OL5081 process.

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.

Yes. OPA obtains information from legacy databases IDRS/CFOL, which includes:

- Taxpayer Identification Number (TIN) – Social Security Number (SSN) and Individual Taxpayer Identification Number (ITIN); ITIN is used for non–US citizens that work and pay taxes in the US
- Personal Identification Number (PIN)
- Caller Identification (CID) – from balance due notice
- Date of Birth (DOB)
- Bank Name
- Bank Address
- Bank Account Name (s) (primary, joint, etc.)
- Type of Account
- Account Address
- Account Number
- Routing Number
- Employer Name
- Employer Address
- Employee Name (primary or secondary)
- Address of record
- Optional phone numbers
- Proposed payment amount
- Payment month or date
- Payment option (pay now, extension or installment agreement)
- Adjusted Gross Income (AGI) from prior year returns
- The Security and Communication System (SACS) – records all access of the mainframe databases. It ensures that the user is a valid user that the user is permitted to perform the command requested, and the command can be requested from the terminal being used. All Integrated Data Retrieval System (IDRS)/Corporate Files Online (CFOL) command codes are logged to the IDRS/CFOL audit trail.
- The Security Audit and Analysis System (SAAS) will receive OPA transmission of time stamps, TINS, audit trails and any taxpayer updates to the account via Application Messaging and Data Access (AMDAS)/Message and Queues (MQ) Series.

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

Security and Communication System (SACS)

- Authorization to Operate (ATO) – September 28, 2007, expires on September 28, 2010
- Privacy Impact Assessment (PIA) – September 26, 2007, expires on September 26, 2010

Integrated Data Retrieval System (IDRS)

- Authorization to Operate (ATO) – March 10, 2009, expires on March 10, 2012
- Privacy Impact Assessment (PIA) – November 6, 2008, expires on November 6, 2011

Security Audit and Analysis System (SAAS)

- Authorization to Operate (ATO) – June 12, 2007, expires on June 12, 2010
- Privacy Impact Assessment (PIA) – January 27, 2007, expires on January 27, 2010

12. Will other agencies provide, receive, or share data in any form with this system?
No other agencies provide, receive, nor share data in any form with this system.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
A request for records disposition authority for OPA and associated records is currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for OPA inputs, system data, outputs and system documentation (as applicable) will be published in IRM 1.15, exact Records Control Schedule and item number to be determined. IDRS retains logs of all access of taxpayer records. All data and audit information is sent to the SAAS application. SAAS records retention is currently being evaluated by SAAS system owners and when approved, will be incorporated into OPA records requirements.

14. Will this system use technology in a new way?
No. The 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.
No. This system will not be used to identify or locate individuals or groups. OPA is used as a means to pay tax balances owed to the IRS.

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.
No. This system does not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. The system does not have the capability to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. OPA provides the taxpayer the opportunity to respond to any negative determinations. If the taxpayer does not qualify for the Online Payment Agreement, a phone number shall be provided to answer any questions.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No. The system uses session cookies only. The browser cache is cleared for all OPA applet user sessions after 15 minutes of inactivity or when the user closes the web browser. All information that is contained in the session is cleared if the user logs out or times out.

View other PIAs on IRS.gov