

Automated Offers in Compromise (AOIC) – Privacy Impact Assessment

PIA Approval Date: Mar. 10, 2009

System Overview

AOIC is a database that allows monitoring, tracking and controlling of offers in compromise submitted to the IRS. An offer in compromise (offer) is a way for the IRS to recoup a portion of the monies owed to it by taxpayers unable to pay their taxes in full. The taxpayer is then required to meet certain obligations over a period of several years, which are tracked to ensure compliance. Should the proposed offer be rejected, the taxpayer may exercise the right to appeal. The AOIC application is undergoing a major change and the database (DB) is being converted.

Systems of Records Notice (SORN):

- IRS 26.019–Taxpayer Delinquent Account (TDA) 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:

- Taxpayer point of contact (POC) information (complete name, name control, business name, home address, home phone number, and fax number)
- Taxpayer Identification Number (TIN) (Social Security Number (SSN) / Employer Identification Number (EIN))
- Tax module data (including outstanding liabilities, unfiled returns, freeze codes, etc.).
- Income, asset, and expense data
- Offer fee payment
- Tax Increase Prevention and Reconciliation Act (TIPRA) payment amounts
- Offer deposit amount
- Offer amount (including payment terms/conditions)
- Low Income Waiver

B. Employee Data:

- Employee POC information (name, work address, work phone number, and work fax number)
- AOIC employee assignment number
- IRS employee badge number
- Standard Employee Identifier (SEID)
- Legacy Employee login ID (tracked in Remarks/History section of AOIC)

C. Audit Trail:

- SEID
- Login/Logout associated with SEID
- User Actions/Activities associated with SEID
- Failed login attempts
- Date/Time stamp on all captured events
- Access Module Auditing (SEID of administrator who added or deleted a new AOIC user, SEID of added employee to include employee role and level of access granted)

D. Other

- Power of Attorney (POA) or Taxpayer Representative POC Information (name, address, phone number, and fax number)
- POA Centralized Authorization File (CAF) number

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

A. IRS :

1. Individual Master File (IMF) Application – Taxpayer Information:
 - POC information (name, name control, home address, phone number) the information is pulled from the latest tax return filed information or most recent change of address submission.
 - TIN (SSN)
 - Tax module data (including outstanding liabilities, unfiled returns, freeze codes, etc.).
2. Business Master File (BMF) Application – Taxpayer Information:
 - POC information (name, name control, business name, address, phone number, and fax number) the information is pulled from the latest tax return filed information or most recent change of address submission.
 - TIN (EIN)
 - Tax modules with outstanding liabilities (amount of money still owed)
 - Unfiled Returns

B. Taxpayer – Taxpayer Information:

1. Form 656 and Form 656-A
 - POC information (name, address, and phone number)
 - TIN (SSN and EIN)
 - Offer deposit amount
 - Offer amount (including payment terms/conditions)
 - TIPRA payment amounts
 - Low income waiver
2. Form 433-A and Form 433-B
 - Taxpayer income, asset, and expense data
 - Taxpayer information taken from the F656 as stated above.
3. Check or Money Order
 - Offer fee payment

C. Employee:

- Employee POC information (name, work address, work phone number, and work fax number)
- IRS employee badge number
- AOIC employee assignment number
- SEID
- Legacy Employee login ID (tracker in Remarks/History section of AOIC)

D. Other Third Party Sources –POAs or another taxpayer representative can request an offer on behalf of a taxpayer. In this case, the POA and/or taxpayer representative information would be captured:

- POA or Taxpayer Representative POC information (name, address, phone number, and fax number)
- POA CAF number

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

Yes. Taxpayer information maintained and processed within AOIC is required in order to process offers. The AOIC application was designed specifically to aid in the processing of offers; therefore, requesting taxpayer information is mandatory. In addition, all employee data maintained in the application is necessary to ensure only authorized users have access in and out of the application.

4. How will each data item be verified for accuracy, timeliness, and completeness?

Prior to the release of data into the production environment, extensive testing is performed to verify the accuracy, timeliness, and completeness of the data elements. Format masks have been installed for most form fields to indicate that, for example, letters cannot be entered into a numeric data field, such as a phone number or date. Additionally, the application checks to ensure all required data fields are completed before a user can move to the next screen. Drop down menus are utilized throughout the application to minimize the amount of incorrect or invalid data entries. Employee and management inspection is performed on each case during case processing and review. Additionally, closed casework is randomly reviewed for accuracy by independent quality review. All offers with a proposed disposition of acceptance or rejection must be reviewed by an Independent Administrative Reviewer (IAR) using the IAR module of AOIC. The IAR employees will either approve or reject case disposition recommendations. IARs are third party reviewers who ensure every proposed acceptance or rejection of an offer was completed correctly, and a logical and correct decision was made. Information that the taxpayer has submitted can also be verified with supporting documentation, (such as bank statements, mortgage papers, etc.) If a discrepancy is identified in any information provided by a taxpayer or taxpayer representative, the IRS can verify that information with third party sources. For example, there are programs available to check the real estate value of a home. This data can be checked against the information a taxpayer has submitted.

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

No. All data sources have been identified in previous questions.

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

Users must log into the AOIC application to obtain information. Data can then be retrieved and displayed by querying offer numbers or TINs. Additionally, data can be retrieved by querying for name control or case assignment numbers.

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

Yes. Data within the application can be retrieved by TINs, name control, assignment numbers, and offer numbers.

Access to the Data

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

Only IRS employees that have been granted login privileges to AOIC, and have access to the IRS intranet, can use AOIC. IRS employees from the Service and Enforcement organizations, Appeals, Taxpayer Advocate Service, system administrators, database administrators, and developers (read-only access on a limited basis), are granted access to the application. All access and permissions are consistent with user designated roles. All access is granted via the Online 5081 (OL5081) process.

Role: AOIC Program Users

Permission: View, write, modify, and delete data within the application

Role: Access Module Users/Administrators

Permission: Full access (view, write, modify, delete, and can add or remove application users from the system)

Role: IRS Business Community

Permission: View-only access used to perform research and run reports

Role: AOIC Developers

Permission: View-only access (for a limited time only) to aid in fixing any problems identified with the program or database.

Role: System Administrators

Permission: Full access to the application server environment

Role: Database Administrators

Permission: Full access to the application databases and data within

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

User access to the AOIC application is determined via the OL5081 process. If a user requires access to the application, the user submits a request using the OL5081 system. Manager approval is required before the access can be granted. Once a manager approves the request, administrators within the Access application module can perform an additional verification on the user and can then grant the appropriate access level.

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. The following IRS systems share data with the AOIC application:

- Individual Master File (IMF) –IMF provides the AOIC application with taxpayer information such as TINs (more specifically SSNs), name, name control, address, phone number, and tax module data. In addition, AOIC sends IMF different requests to pull tax module data on specific taxpayers identified within the AOIC application.
- Business Master File (BMF) – BMF provides the AOIC application with taxpayer information such as TINs, name, name control, address, phone number, and tax module data. In addition, AOIC sends BMF different requests to pull tax module data on specific taxpayers identified within the AOIC application.
- Standardized IDRS Access Tier II (SIA Tier II) –TINs and tax module data are shared between the two systems. AOIC provides this data to SIA Tier II to be uploaded to IDRS. In return, AOIC receives a negative or positive indicator (regarding the status of the data upload) from IDRS via SIA Tier II.
- Appeals Centralized Database System (ACDS) – The ACDS sub-system eCase interfaces with AOIC to check for any matching offer records that exist in the AOIC database. The eCase check is completed against the AOIC database using offer numbers or TINs (SSN or EIN) that exist in the eCase sub-system of ACDS. Matching AOIC offer records found by eCase are extracted to the eCase sub-system of ACDS. Offer numbers, TINs (SSN or EIN), and tax module data are obtained by eCase on a read-only basis.

- Collection Information System (COINS) – AOIC sends statistical data (such as number of open and closed cases, etc.) to the COINS application for generation of SB/SE Collection reports. No PII data is shared between these two systems.

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

Yes.

Individual Master File (IMF)

- Certification & Accreditation (C&A)–June 21, 2007, expires June 21, 2010
- Privacy Impact Assessment (PIA)–June 7, 2007, expires June 7, 2010

Business Master File (BMF)

- Certification & Accreditation (C&A)–June 14, 2007, expires June 14, 2010
- Privacy Impact Assessment (PIA)–April 10, 2007, expires April 10, 2010

Standardized IDRS Access Tier II (SIA Tier II)

- Certification & Accreditation (C&A)–June 19, 2008, expires June 19, 2011
- Privacy Impact Assessment (PIA)–March 28, 2008, expires March 28, 2011

Appeals Centralized Database System (ACDS)

- Certification & Accreditation (C&A)–April 18, 2008, expires April 18, 2011
- Privacy Impact Assessment (PIA)–January 10, 2008, expires January 10, 2011

Collection Information System (COINS)

- Certification & Accreditation (C&A)–June 2, 2006, expires June 2, 2009
- Privacy Impact Assessment (PIA)–April 14, 2006, expires April 14, 2009

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

No. The AOIC application interfaces and shares data solely with IRS internal systems. The Treasury Inspector General for Tax Administration (TIGTA) and Government Accountability Office (GAO), however, may request data files or certain reports be generated.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

In accordance with IRM 1.15.2.3, AOIC data is considered permanent records, as identified by National Archives and Records Administration (NARA). The data contains significant historical value warranting its continued preservation. Data retention is not less than is required by the Code of Federal Regulations (CFR) 4.804-5 and NARA. At this point, nothing has been archived. All data maintained in the application since its initial deployment is stored in different tables within the application. AOIC data records are maintained in accordance with Records Disposition Handbooks, IRM 1.15.2.1 through IRM 1.15.2.3.

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

No. The AOIC application 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. The AOIC application is not used to identify or locate individuals or groups of people.

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 physical monitoring is possible. Individual activities within the system are monitored for adherence to policy and controls, and detection of suspect activity. This information is used for tracking user activity within the system. In addition, the AOIC application monitors a taxpayer's offer request. After an offer is originally submitted by a taxpayer, the offer is assigned an identification number and is tracked within the AOIC application until a disposition decision has been made. After a decision is made that is agreed upon by all parties, the offer can be closed. The offer is never deleted from the system and can be researched at any time. However, once closed, an offer is no longer actively tracked or monitored.

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

No. Although certain data stored within the application suggests a taxpayer may be treated differently by the IRS (for example whether or not a taxpayer offer is accepted), the system does not make any of these determinations. Decisions are made by employees who have researched each offer case. An accepted offer will allow taxpayers to pay various tax dollars regarding their specific offer request. The overall treatment to each taxpayer, however, will not differ. Therefore, the use of the AOIC application does not allow the IRS to treat taxpayers, employees, or others disparately.

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

Yes. If an offer submitted by a taxpayer is rejected, the taxpayer has thirty (30) days to appeal the decision. The request for an appeal comes to the offer group and is forwarded to Appeals to make a final determination. In addition, AOIC personnel can reverse their decision if the taxpayer can provide additional information sufficient to support changing the rejection decision (as long as it is within 30 days).

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

No. AOIC is web-based; however, persistent cookies or other tracking devices are not used to identify web visitors.

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