Electronic Installment Agreement (eIA) – Privacy Impact Assessment

PIA Approval Date – Dec. 11, 2006

Requested Operational Date – Currently in the operational and maintenance phase.

System Overview

The Electronic Installment Agreement (eIA) applet will provide taxpayers that owe money to the IRS the capability of setting up an installment plan via the Web interface offered through eIA. eIA will allow the taxpayer or an authorized representative (Power of Attorney) to apply for and receive online approval for a short term extension of time to pay or set up a monthly installment agreement. Taxpayers will also have the option of paying the full amount of the balance due.

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 may include the following:

- 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
- 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)
- Pre-assessed taxpayers have to provide their adjusted gross income from prior tax returns

B. Audit Trails: The system 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, eIA sends all of its business layer outbound responses to Security Audit and Analysis System (SAAS) through Application Messaging and Data Access Services (AMDAS) on the outbound queue.

C. Other: Power of Attorney (POA's) users can access eIA by first providing a combination of his/her Centralized Authorization File (CAF) number, taxpayer's Caller ID, and SSN/ITIN from the taxpayer's balance due notice.

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 the Integrated Data Retrieval System (IDRS) 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 using command codes (which includes TIN, PIN, CID, DOB, Address of Record, entity and module data).

B. Taxpayer: The personally identifiable information that taxpayers may submit on-line in order to fulfil their payment obligation to the IRS is referenced in question 1A of this PIA.

C. State and Local Agencies: The IDRS process does not directly share any data with state or local agencies. Data that is processed by IDRS and then sent to the Masterfile is however shared with State and Local Governments as part of the Federal -State Relations Project.

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 eIA.

4. How will each data item be verified for accuracy, timeliness, and completeness?
eIA restricts user input through the use of multiple mechanisms. The eIA applet restricts user input through the use of JavaScript 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. eIA 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.

eIA 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. eIA receives data from taxpayers and no other sources.

6. Generally, how will data be retrieved by the user?
Data will be retrieved from IRS records by the user through the publicly available Web front end portion of the application using a standard 128-bit Secure Sockets Layer (SSL) encryption capable Web browser such as Internet Explorer or Netscape Navigator. Users will have no direct access to IRS systems beyond the front end Web server. Users shall only have such access to the Web server as is necessary to provide eIA 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 eIA are required to authenticate prior to being granted access to the applet. Each taxpayer must enter a PIN that is used in combination with TIN/SSN for user authentication. No access to the eIA applet is allowed without first authenticating. If a taxpayer does not have a PIN, the taxpayer can click on the link "Create a PIN" to establish a PIN using his/her SSN/ITIN or "Forgot a PIN" to re-establish a PIN, or s/he may enter the Caller ID number from their balance due notice and their date of birth.

POA user will need to authenticate using a combination of the taxpayer's Caller ID, SSN/ITIN from the taxpayer's balance due notice, and the POA's CAF number. After authentication, the POA can access the eIA applet.

All pre-assessed taxpayers must enter their SSN/ITIN, spouse's SSN/ITIN (if joint return), DOB and the adjusted gross income from their last years tax return.

Each POA user on a pre-assessed return must enter the taxpayer's SSN/ITIN, the taxpayer's spouse's SSN/ITIN (if joint return), the taxpayer's adjusted gross income from their last years tax return and the POA's 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 (SA's) have access to the production Oracle database that will hold the taxpayer entered data (behind the 3rd firewall) if the taxpayer chooses to save their progress within the eIA Web-based application before completing the payment agreement in order to finish the online payment agreement at a later date/time. An automatic data removal process occurs every two weeks.

If the taxpayer does not save his/her progress in the system, the data is removed from the eIA Web-based application when the Web Sphere session times out. There is no other persistent data in eIA.

Currently, eIA has a contractor that holds the role as an Oracle Database Administrator.

9. How is access to the data by a user determined and by whom?
To ensure only authorized personnel are accessing eIA and that secure information is not maliciously altered or unintentionally modified, System Administrators responsible for assigning permissions ensure that the proper permissions are granted to the proper users. All policy and procedures are followed in granting users permissions, determining permissions; ensuring user rights are restricted to the minimum necessary to perform the job, background screening and separation of duties.

Each IRS position designation is documented on the Standard Position Description (SPD) and assigned a risk level (or sensitivity level) commensurate with the sensitivity of the information, the risk to that information and the system maintaining that information. Three levels of risk have been designated by the IRS for employee and contractor positions with each level requiring a more rigorous background investigation.

Re-investigations are conducted every 5 years for high-risk, Top Secret and Contractor clearances.

Contractor personnel who will be granted staff-like access to IRS facilities, Information Systems, Security Information, Strategic Business Systems or Sensitive IRS information Systems, are required

to undergo a Security Screening Investigation (SSI) unless a Task Order specifies elsewhere that another type of investigation is more suitable to the circumstances.

The current Database Administrator Contractor obtained a Department of Treasury Security Clearance after completing and submitting a Minimum Background Investigation packet prior to being granted access to IRS systems.

The IRS has implemented an automated, formalized process for user account administration using the OL5081 system. The OL5081 process requires confidential security agreements for employees assigned to work with both sensitive and non-sensitive information. All new users requesting access to an IRS system must do so through the OL5081 system.

Once a user has been approved for access to the system by managers, OL5081 will email an approval notification to the user. The user must then log onto OL5081, read and agree to the Security Rules.

The OL5081 allows eIA managers to assign only need-to-know permissions to each developer. Based upon the permissions assigned to a specific group, the developer then has access to perform development activities in eIA. Permissions are granted according to the group the individual will be working for.

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. IDRS is a system consisting of databases and operating programs (subsystems) that support IRS employees working active tax cases within each business unit across the entire IRS. This application manages data that has been retrieved from the Tax Master Files allowing IRS employees to take specific actions on taxpayer account issues, track status and post transaction updates back to the Master File. It provides for systemic review of case status and notice issuance based on case criteria, alleviating staffing needs and providing consistency in case control.

The personally identifiable information that taxpayers may submit on-line in order to fulfill their payment obligation to the IRS is indicated in question 1A of this PIA.

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

- C&A approved on May 18, 2006, expiring May 18, 2009
- Privacy Impact Assessment approved on March 22, 2006, expiring March 22, 2009.

12. Will other agencies provide, receive, or share data in any form with this system?
No other agencies provide, receive, or 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?
When taxpayers save unfinished sessions, that data is retained on a special data server behind a third firewall. An automatic data removal process occurs every two weeks.

Regarding audit log data that is archived, audit logs may be retained up to seven (7) years, per IRM 1.15, Records Management.

14. Will this system use technology in a new way?
No.

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. eIA 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?
No.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. Taxpayers that owe money to the IRS will be able to access eIA from the IRS home page and review the eligibility requirements for the installment agreement. Taxpayer's that are deemed not eligible for the installment agreement are provided with a number to call in.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. eIA provides the taxpayer the opportunity to respond to any negative determinations. If the taxpayer does not qualify for the Electronic Installment 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 eIA applet user sessions after twenty minutes of inactivity or when the user closes the Web browser. All information that is contained in the session is cleared.

View other PIAs on IRS.gov