NOTE: The following reflects the information entered in the PIAMS Website.

A. SYSTEM DESCRIPTION


Date of Approval: 07/15/2014  PIA ID Number: 1002

1. What type of system is this? Modernized System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

   Modernized Internet Employer Identification Number, MOD-IEIN

2a. Has the name of the system changed? No
   If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

   Number of Employees: Not Applicable
   Number of Contractors: Not Applicable
   Members of the Public: Not Applicable

4. Responsible Parties: NA

5. General Business Purpose of System

   Modernized Internet Employer Identification Number (Mod IEIN) is part of the Integrated Customer Communications Environment Web Applications (ICCE Web Apps). Mod IEIN will help taxpayers, businesses, and their representatives complete the application for Employer Identification Number (EIN), Application for Employer Identification Number (Form SS-4), using a new interactive system which asks questions tailored to the type of entity the taxpayer is establishing. By providing full automation of the back-end processing of EIN assignment, the applet will eliminate the assignment of "provisional" EINs, resulting in improved ease of receiving valid and ready-to-use EINs. The Mod IEIN web application will also improve overall processing accuracy and timeliness, additionally allowing IRS telephone assistants to devote time to more productive activities. Currently, 80% of taxpayers who qualify for an EIN are able to secure EIN approval and initiation via IRS.gov. Due process is provided pursuant to 26 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact *Privacy and request a search) Yes

   6a. If Yes, please indicate the date the latest PIA was approved: 05/13/2010

   6b. If Yes, please indicate which of the following changes occurred to require this update.

      - System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
      - System is undergoing Security Assessment and Authorization Yes

   6c. State any changes that have occurred to the system since the last PIA

      Re-Authorization. Eliminated the download of information to TTB (Tax and Trade Bureau). Added Name Control language to CP 575. Check for Date of Death on responsible party TINs. Change in hours of operation. One stop added state of Virginia.

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XXX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management
8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

<table>
<thead>
<tr>
<th>Category</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taxpayers/Public/Tax Systems</td>
<td>Yes</td>
</tr>
<tr>
<td>Employees/Personnel/HR Systems</td>
<td>No</td>
</tr>
<tr>
<td>Other Source</td>
<td>No</td>
</tr>
</tbody>
</table>

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

<table>
<thead>
<tr>
<th>TYPE OF PII</th>
<th>Collected?</th>
<th>On Public?</th>
<th>On IRS Employees or Contractors?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Social Security Number (SSN)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Tax Payer ID Number (TIN)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Address</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Additional Types of PII: No

No Other PII Records found.

10a. Briefly describe the PII available in the system referred to in question 10 above.

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

Treas. Reg. section 301.6109-1(d)(2) provides, "[a]ny person required to furnish an employer identification number must apply for one, if not done so previously on Form SS-4....The form, together with any supplementary statement, must be prepared and filed in accordance with the form, accompanying instructions, and relevant regulations, and must set forth fully and clearly the requested data."

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

Truncation of Social Security Number (last four digits masked)

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

None, a Social Security Number is needed to obtain an EIN
11. Describe in detail the system’s Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an Audit Trail is not needed.

Mod IEIN Audit Data is captured by the Security Audit and Analysis System (SAAS). Audit Trail logging for the applet is sent to SAAS via Application Messaging and Data Access Services (AMeDAS) for each transaction that reaches the back-end.

- Entity Type (e.g., sole proprietor, partnerships, corporations, Limited Liability Company, estate, withholding agent, household employer, political organization, receivership)
- A Limited Liability Company Check
- A Reason for Applying
- Name (Company Name or First/Middle/Last/Suffix)
- Social Security Number (SSN) / Individual Taxpayer Identification Number (ITIN) / Employer Identification Number (EIN)
- Third Party Designee Check (If the person completing the application is a third party acting on behalf of the taxpayer, we can’t provide the 3rd party with the online notice. Therefore, we determine if the person is the actual taxpayer or a Third party to determine what actions to take when we assign the EIN. Name of Third Party Designee (if applicable) (First/Middle/Last/Suffix)
- “Care Of” Name (Used in the event the taxpayer would like his/her mail addressed to a different person/business, such as a secretary or office manager.)
- Physical Location Street City State/US Territory Zip Code Phone Number
- Mailing Address (if applicable) Street City State/US Territory Country Zip Code
- Third Party Designee Address (if applicable) Street City State/US Territory Zip Code Phone Number
- Legal Name
- Trade Name (Used by companies who advertise their business name as something different than their legal name.)
- County where business is located
- State where business is located/incorporated
- Date Business Started/Acquired or Date of Death
- Closing Month of Accounting Year
- Principal Business Activity (A business activity represents tangible goods, such as automobiles.)
- Principal Service Activity (a service activity represents intangibles, such as consulting.)
- Employee Hired Check
- Employee Information on employees that receive W2s (rather than 1099s) (if applicable) Wages Paid Date Number of Agricultural Employees Number of Household Employees (only for certain types) Number of Other Employees Employment Tax Liability Information
- Number of Members in Limited Liability Company (LLC)
- Corporation or Sub Chapter S Check (Corporations have the option to be classified as a regular corporation or a Sub Chapter S corporation (S-Corp). If a company wants to be an S-Corp, they must file a form requesting this classification, which we tell them about if we determine they want
to be an S-Corp. This check is used to determine if we need to provide them with the S-Corp information.)

- EIN Confirmation Letter Delivery preference
- Trustee business name/trustee individual name
- Type of real estate investment trust (mortgage or equity) The SSN and name control of the Taxpayer are required as part of the authentication process and cannot be substituted by another data field to identify the customer. The information is captured for Audit Trail purposes. Even though a ready-to-use EIN is being issued, the IRS still needs to have the ability to have Audit Trails for future reference if necessary. These are for internal use and are closely guarded. They are only available to IRS employees who follow the proper procedures to gain access to them, which is by going through the OL5081 process. A manager must approve the OL5081 request and then an administrator will grant the access.

11a. Does the Audit Trail contain the Audit Trail elements as required in current IRM 10.8.3 Audit Logging Security Standards? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:
   a. IRS files and databases: Yes
      If Yes, the system(s) are listed below:
      | System Name | Current PIA? | PIA Approval Date | SA & A? | Authorization Date |
      |-------------|--------------|-------------------|---------|-------------------|
      | IDRS        | Yes          | 06/30/2014        | Yes     | 12/09/2011        |

   b. Other federal agency or agencies: No
      If Yes, please list the agency (or agencies) below:

   c. State and local agency or agencies: No
      If Yes, please list the agency (or agencies) below:

   d. Third party sources: No
      If yes, the third party sources that were used are:

   e. Taxpayers (such as the 1040): Yes
   f. Employees (such as the I-9): No
   g. Other: No If Yes, specify:

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

The Mod IEIN application provides Taxpayers, businesses, and their representatives with an option to complete the application for Employer Identification Number (EIN), Application for Employer Identification Number (Form SS-4), using a new interactive system which asks questions tailored to the type of entity the taxpayer is establishing. By providing full automation of the back-end processing of EIN assignment, the applet eliminates the assignment of “provisional” EINs, resulting in improved ease of receiving valid and ready-to-use EINs. The Mod IEIN web application improves overall processing accuracy and timeliness, additionally allowing IRS telephone assistors to devote time to more productive activities. All PII gathered in the course of the application is used to fulfill the requirements of the application for EIN. Treas. Reg. section 301.6109-1(d)(2) provides, "[a]ny person required to furnish an employer identification number must apply for one, if not done so previously on Form SS-4....The form, together with any supplementary statement, must be prepared and filed in accordance with the form, accompanying instructions, and relevant regulations, and must set forth fully and clearly the requested data."
14. **What is the specific use(s) of the PII?**

<table>
<thead>
<tr>
<th>Use</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>To conduct Tax Administration</td>
<td>Yes</td>
</tr>
<tr>
<td>To provide Taxpayer Services</td>
<td>Yes</td>
</tr>
<tr>
<td>To collect Demographic Data</td>
<td>No</td>
</tr>
<tr>
<td>For employee purposes</td>
<td>No</td>
</tr>
</tbody>
</table>

*If other, what is the use?*
E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.)  Yes

15a. If yes, with whom will the information be shared? The specific parties are listed below:

<table>
<thead>
<tr>
<th>Other federal agency (-ies)</th>
<th>Yes/No</th>
<th>Who?</th>
<th>ISA OR MOU??</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Administration and Census</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| State and local agency (-ies) | No |
| Third party sources | No |
| Other: | No |

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public?  Yes

17. Does the website use any means to track visitors’ activity on the Internet?  Yes

If yes, please indicate means:

<table>
<thead>
<tr>
<th>YES/NO</th>
<th>AUTHORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent Cookies</td>
<td>No</td>
</tr>
<tr>
<td>Web Beacons</td>
<td>No</td>
</tr>
<tr>
<td>Session Cookies</td>
<td>Yes</td>
</tr>
<tr>
<td>Other:</td>
<td>No</td>
</tr>
</tbody>
</table>

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information?  Yes

18a. If Yes, how is their permission granted?

The MOD IEIN web application provides users with confirmation pages for consent and displays notifications throughout the process. The user may decline consent and exit the application at any time and all information not submitted is immediately destroyed upon termination of the application.

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

19a. If Yes, how does the system ensure “due process”?

If there is an error during processing, the system displays an error code to the user and provides instructions on how to submit an SS-4 EIN application. The only way for an individual to change his/her application data once it has been processed is to submit a request in writing.

20. Did any of the PII provided to this system originate from any IRS issued forms?  No

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent  Yes
Website Opt In or Out option  Yes
Published System of Records Notice in the Federal Register  Yes
Other:  No
G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

<table>
<thead>
<tr>
<th>IRS Employees:</th>
<th>Yes/No</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Yes</td>
<td>No Access</td>
</tr>
<tr>
<td>Managers</td>
<td></td>
<td>No Access</td>
</tr>
<tr>
<td>System Administrators</td>
<td></td>
<td>Read Write</td>
</tr>
<tr>
<td>Developers</td>
<td></td>
<td>Read Write</td>
</tr>
<tr>
<td>Contractors:</td>
<td>Yes</td>
<td>Read Write</td>
</tr>
<tr>
<td>Contractor Users</td>
<td></td>
<td>Read Write</td>
</tr>
<tr>
<td>Contractor System Administrators</td>
<td></td>
<td>Read Write</td>
</tr>
<tr>
<td>Contractor Developers</td>
<td></td>
<td>Read Write</td>
</tr>
<tr>
<td>Other:</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

If you answered yes to contractors, please answer 22a. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have “Root Access”, does that person hold a properly adjudicated “High Level” background investigation? Yes

23. How is access to the PII determined and by whom?

Users provide PII to the system by inputting information (as listed in 10a) through MOD IEIN. The collected PII from the current session is displayed to the user. Upon submission, PII is submitted and committed to the IRS IDRS/ERAS systems, on the web interface that data is destroyed. Once the Taxpayer submits the information on the Mod IEIN web application and that information passes up-front validity checks, the Taxpayer will receive either a successfully generated EIN or an error message, which reads “The information you have entered does not match IRS records.” The applicant will be able to view the information screen by screen, but will not be allowed to change the information on most of the screens once he/she advances to the next screen. However, a summary page will be shown with the information entered, but the Taxpayer will not be able to make changes unless they start the process over. IRS employees will not play a role, unless Taxpayer is unable to properly authenticate and receive an error message to contact IRS for assistance, at which time the Taxpayer provides written information for IRS employees to input manually. Once the Taxpayer submits the information on the Mod IEIN web application and the information passes up-front validity checks, the information will then run through the backend validation process and post automatically, provided all the information matches IRS records. If the information does not match IRS records, it will be rejected back to the taxpayer for correction and re-submission. Data is not retrievable from Mod IEIN by a personal Identifier such as name, SSN, or other unique Identifier since Mod IEIN is not a database. Taxpayers will not be able to access their data once they’ve submitted it. After submission or completion of an application, data can be retrieved from IDRS only by an IRS employee using personal identifiers such as name of the entity or EIN and mailing address that was used to apply for an EIN on a need to know basis.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

The validation process will verify the accuracy and completeness of the information in accordance with the business rules. It is worth noting that the only validation Mod IEIN performs is a validation of the Taxpayer’s TIN and name control (business or individual) against IRS records in Integrated Data Retrieval System (IDRS) to authenticate the applicant. Mod IEIN passes the TIN entered by the Taxpayer to IDRS. IDRS returns the individual’s name control that is on file for the entered TIN, if found. Mod IEIN confirms that the individual name control provided by the taxpayer matches the name control returned from IDRS and that an existing EIN does not exist under said TIN. If the information matches IRS records and no duplicate EIN exists, the record will post to IDRS immediately. If the information does not match IRS records, the record will reject back to the taxpayer for correction and re-submission.
If the Taxpayer cannot correct the information within three attempts, he/she will be given an error page and their session will end. He/she will then have to start the online process again to be able to submit the application. The system will provide TIN based authentication to limit the user to 5 failure counts within a day to authenticate with the same TIN (SSN/ITIN/EIN) and name based authentication. The system will look for an exact match for the individual name control or business name control. Addresses are verified using the Integrated Customer Communications Environment (ICCE) Finalist interface, an approved United States Postal Service (USPS) system. However, Finalist is only used in order to change addresses into the USPS approved format (i.e. A nine-digit zip code instead of just five-digit). Only accepting those applications that pass all validation checks and forcing the taxpayer to provide correct information up-front guarantees 100% automation, accuracy, timeliness, and completeness.

25. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

25a. If Yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

All data relating to Applications for MOD IEIN will be retained in accordance with disposition instructions published in Document 12990 under Records Control Schedule (RCS) 29, item 70. Data submitted on individual applications will not be retained for any period of time in Mod IEIN; the information will post directly to IDRS. However, invalid authentication attempts on the application will be stored in the Mod IEIN authentication database for the remainder of that day. The Mod IEIN application will execute a script that purges and overwrites the data to ensure its deletion. It should be noted that this database maintains invalid authentication attempts so that users are limited to a certain number of invalid authentication attempts per day. In addition to the Mod IEIN authentication database that retains invalid authentication attempts, the IRS will provide, store, and catalog the assignment of EINs posted to the Master File via ERAS. The Master File is the location where EIN information is stored for official IRS record-keeping purposes.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

Admin: OL5081, tech ctrls: firewall, no data stored

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

No data saved/stored on system

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

MOD-IEIN sends security audit records to SAAS on a continuous basis and meets or exceed IRS & FISMA requirements for security.
29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? No

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

<table>
<thead>
<tr>
<th>SORNS Number</th>
<th>SORNS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treas/IRS 24.046 BMF</td>
<td>BMF</td>
</tr>
<tr>
<td>Treas/IRS 34.037 IRS Audit Trail and Security Records System</td>
<td></td>
</tr>
</tbody>
</table>

Comments
I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

   - Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)   | No
   - Provided viable alternatives to the use of PII within the system    | No
   - New privacy measures have been considered/implemented    | No
   - Other:                                                      | No

32a. If Yes to any of the above, please describe:

   Not Applicable

View other PIAs on IRS.gov