

Date of Approval: **March 11, 2019**

PIA ID Number: **3901**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

United States Residency Certification, US CERT

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

United States Residency Certification, US CERT, PIA ID # 1656

What is the approval date of the most recent PCLIA?

3/9/2016

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

It belongs to the Security Change Management Review Board (SecChM).

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The US CERT application automates much of what was a pure paper process, thereby providing requestors of Form 6166 faster, quality service by eliminating many of the steps found in IRS paper processing. Though the taxpayer (or third party on behalf of the taxpayer) must still submit a paper request (Form 8802) and receive a paper certification (Form 6166), data storage and validation of that taxpayer data is done electronically in a single database. Once a valid Form 8802 request is input into the database by an input operator, it is often certified without human intervention through automated Integrated Data Retrieval System (IDRS) research. Where requests requiring further attention or manual research, the business unit employees are able to track and work these requests within the database application until either they are rejected or certified. Hence, the application provides a variety of rejection and suspense letters, as well as various managerial reports of an inventory and statistical nature.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Delivery of governmental benefits, privileges, and services

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

SSNs are needed in order to verify fact of filing due to the taxpayer requesting F6166 letters to offset foreign taxation.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

This relates to the SSN/EIN planned mitigation. The Office of Management and Budget memorandum M-17-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. U.S. Certs requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

Standard Employee Identifier (SEID)

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Are there other types of SBU/PII used in the system?

No

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The US CERT application collects and verifies all information for the process of approving (or denying) taxpayers F6166 letters to offset foreign taxation.

How is the SBU/PII verified for accuracy, timeliness and completion?

The information is verified against Integrated Data Retrieval System (IDRS) to determine accuracy.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Integrated Data Retrieval System (IDRS)

Current PCLIA: Yes

Approval Date: 10/1/2018

SA&A: Yes

ATO/IATO Date: 10/14/2018

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 6166 Form Name: Certification of U.S. Residency

Form Number: 8802 Form Name: Application for U.S. Residency Certification

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

The information is not collected directly from individuals. The information collected as part of the application is the information obtained from various IRS databases and files, which in turn are tax forms filed by tax entities. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

If the application is not complete with all the required information, then we cannot process their application and issue them the US Residency Certification they are requesting. The information is not collected directly from individuals. The information collected as part of the application is the information obtained from various IRS databases and files, which in turn are tax forms filed by tax entities. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

Periodic (30, 60 day) letters are sent (automatically, by the system) requesting information lacking, to render a determination. The information is not collected directly from individuals. The information collected as part of the application is the information obtained from various IRS databases and files, which in turn are tax forms filed by tax entities. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

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

Management of the US CERT group (user group) assigns access levels to the various Tax Examiners (TEs), clerks, etc. A potential user will request access via the Online 5081 system. This request must be approved by the potential user's manager based on a user's position and need-to-know.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

U.S. CERT data for accepted or rejected applications is approved for destruction 10 years after case is closed. The National Archives/Archivist of the United States approved this data retention under Job No. N1-058-08-4 (signed 3/3/2008). The dispositions of system input and output records, as well as system documentation records are also covered under that job number. System outputs and documentation are approved for destruction when superseded or no longer needed. However, paper input record Form 8802, must be retained for 6 years and 3 months after calendar year in which related case is closed. All records disposition instructions for U.S. CERT are published in IRS Document 12990, under Records Control Schedule 29 for Tax Administration - Wage and Investment, Item 418.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

2/2/2016

Describe the system's audit trail.

The system records the input OP (SEID) as well as a timestamp (various) for any Database entry on the record itself.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Test results are stored in TFIMS (Treasury FISMA Inventory Management System).

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

ASCA has been completed and include Privacy Controls.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?

No