Date of Approval: **April 10, 2023**

PIA ID Number: **7763**

SYSTEM DESCRIPTION

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

Project: FTC delivery of identity theft data to IRS, 14039-SDT

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?

Project: FTC delivery of identity theft data to IRS, 14039-SDT, PIA#5253

What is the approval date of the most recent PCLIA?

6/23/2020

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.

WI-CAS-AM-Identity Protection Strategy & Oversight staff in partnership with other Fed agency, the Federal Trade Commission (FTC)

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?

No

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 business purpose, caused by Executive Order 13681, mandates the Federal Trade Commission (FTC) and other agencies improve the Security of Consumer Financial Transactions and to enhance Identity Theft Remediation. Section 2 of EO 13681, requires the reduction of burden on consumers who've been victims of identity theft, including substantially reducing the amount of time necessary for a consumer to remediate typical incidents such as tax-related identity theft. The FTC will transmit completed Forms 14039 (Identity Theft Affidavit) for victims that opt-in to have FTC share it with the IRS. The IRS will process the Forms 14039 as they do all other Forms 14039. The benefit to victims is reduced burden in reporting and decreased recovery time. This also accomplishes improved victim assistance response time on behalf of the IRS.

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:

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).

The SSN is needed and required on Form 14039 to accurately and efficiently identify a victim's record. The "FTC delivery of identity theft data to IRS, 14039-SDT" system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

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

Mitigation methods will follow that of the 1040 suite's application of SSN-ER. The SSN is needed and required on Form 14039 to accurately and efficiently identify a victim's record. The "FTC delivery of identity theft data to IRS, 14039-SDT" system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

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
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:

Protected Information - Information which if modified, destroyed, or disclosed in an unauthorized manner could cause loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.

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 PII needed in this system allows employees to evaluate, process and apply appropriate actions based upon the information contained in the Form 14039. The application requires the SSN to enable accurate research of affected tax accounts of identity theft victims.

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

Individuals utilize the FTC's IdentityTheft.gov website to report they are identity theft victims and opt-in via the FTC site to request the FTC to forward their Form 14039 to the IRS. The FTC site utilizes two-factor authentication. The IRS Form 14039 is reviewed by the victim / individual prior to saving their information on the FTC server and in so doing confirm its present accuracy. The Form 14039 explains the rights of the individual and their FTC-provided authentication confirms their identity, however IRS Identity Theft Victim Assistance (IDTVA) 'customer service representatives' scrutinize all Forms 14039 in all manner of delivery and always evaluate their validity and accuracy. When working with the victim the Customer Service Representative (CSR) will accept and consider additional or revised information provided by the victim. Forms 14039 are processed individually by the IRS. The IDTVA CSR utilizes the evidence provided by the victim and when the tax account is impacted, they utilize information relative to that. As a victim of fraud, it's imperative the information provided be correct and verified by IRS in order to determine case next steps and resolution.

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

IRS 42.021 Compliance Programs and Projects Files

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?

No

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

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: Federal Trade Commission
Transmission Method: Secure Data Transfer (SDT) IRS Safeguards
ISA/MOU: Yes

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: 14039
Form Name: IRS Identity Theft Affidavit

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?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

IRS does not collect the information directly from the victim. FTC's identitytheft.gov collects the info and utilizes 'opt-in' process to confirm a victim (individual) voluntarily wants FTC to

provide specific complaint data that's collected in fields of an IRS Form 14039. The full Privacy Notice is also provided on the Form 14039.

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):

This 'opt-in' and 'opt-out' functionality is housed on the FTC website, identitytheft.gov.

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

The Form 14039 explains the rights of the individual and their FTC-provided authentication confirms their identity, however IRS Identity Theft Victim Assistance CSRs scrutinize all Forms 14039 in all manner of delivery and always evaluate their validity and accuracy. When working with the victim the CSR will accept and consider additional or revised information provided by the victim.

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 Only

System Administrators: Administrator

Developers: Read Write

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

The data provided by FTC is transmitted to IRS using Governmental Liaison (GL)'s Secure Data Transfer (SDT) and it resides on a secure IRS server. Access to the server is administered via Business Entitlement Access Request System (BEARS) requests and is

granted by the IRS Identity Protection Strategy and Oversight (IPSO) office Subject Matter Expert (SME) on a 'need-to-access' basis. An IPSO based SME will oversee server access. There are only four IRS employees with access to the server at any time, one primary point of contact (POC) in IPSO and their backup.

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.

All records housed in the 14039SDT system are erased / purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS Records Control Schedule (RCS) 11, Item 15 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. RCS 29 Item 56-Income Tax Returns Filed by Individuals, Partnerships and Fiduciaries/(c) Filed with returns in potential refund litigation case files. Returns and all related documents. RCS 29 Item 439 (A) or (B)-Fraudulent Tax Scheme Files. RCS 29 Item 446-IRS Identity Validation (Out of Wallet) System RCS 28 Item 6(a)-Case Files. National Fraud Program Case Files

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

Each file FTC transmits to IRS is assigned a unique identifier by FTC. GL-Safeguards Secure Data Transfer process will track IRS receipt and confirmation actions and email confirmations via the mailbox that reference the 'identifier' in the subject line.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

It's not an IRS system.

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: Not Applicable

Contractors: Not Applicable

Members of the Public: Under 100,000

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