

---

**A. SYSTEM DESCRIPTION**

---

1. 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

2. Is this a new system? Yes

2a. If **no**, is there a PIA for this system?

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Next, enter the **date** of the most recent PIA.

Indicate which of the following changes occurred to require this update (check all that apply).

<u>No</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	Internal Flow or Collection

Were there other system changes not listed above?

If yes, explain what changes were made.

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>No</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>Yes</u>	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

---

**A.1 General Business Purpose**

---

5. 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 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.

---

**B. PII DETAIL**

---

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes    On Primary            Yes    On Spouse            Yes    On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
No	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (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. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	No	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	Yes

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
No	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

---

## **B.1 BUSINESS NEEDS AND ACCURACY**

---

7. 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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

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 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.

---

## **C. PRIVACY ACT AND SYSTEM OF RECORDS**

---

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **other**, explain your answer.

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

<u>SORNS Number</u>	<u>SORNS Name</u>
Treas/IRS 24.030	IMF
Treas/IRS 24.046	BMF
Treas/IRS 42.021	Special Programs and Project Files

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

---

#### **D. RESPONSIBLE PARTIES**

---

10. Identify the individuals for the following system roles. # # Official Use Only

---

#### **E. INCOMING PII INTERFACES**

---

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? No

11b. Does the system receive SBU/PII from other federal agency or agencies? Yes

If **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).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
Federal Trade Commission	Secure Data Transfer (SDT) IRS Safeguards	Yes

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

<u>Form Number</u>	<u>Form Name</u>
14039	IRS Identity Theft Affidavit

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

---

## F. PII SENT TO EXTERNAL ORGANIZATIONS

---

12. Does this system disseminate SBU/PII? No

12a. Does this system disseminate SBU/PII to other IRS Systems?

---

## G. PRIVACY SENSITIVE TECHNOLOGY

---

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

---

## H. INDIVIDUAL NOTICE AND CONSENT

---

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

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?

IRS does not collect the information directly from the victim. FTC's [identitytheft.gov](http://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.

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

18a. If **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](http://identitytheft.gov).

19. 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.

---

**I. INFORMATION PROTECTION**

---

20. 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

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

IRS Employees? Yes

<u>IRS Employees?</u>	<u>Yes/No</u>	<u>Access Level (Read Only/Read Write/Administrator)</u>
Users	Yes	Read and Write
Managers	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	Yes	Read And Write

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? The data provided by FTC is transmitted to IRS using GL's SDT and it resides on a secure IRS server. Access to the server is administered via 5081 requests and is granted by the IRS 'Identity Protection Strategy and Oversight' office SME on a 'need-to-access' basis. The 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' in IPSO and their backup; and one primary POC in Fresno IDTVA and their backup.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act? Not Applicable

---

**I.1 RECORDS RETENTION SCHEDULE**

---

22. 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

22a. 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 records housed in the 14039SDT system will be erased or 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.

---

**I.2 SA&A OR ECM-R**

---

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the system's audit trail. Each file FTC transmits to IRS will be 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, "\*\*W&I CAS:AM:IPSO-FTC" that reference the 'identifier' in the subject line.

---

## **J. PRIVACY TESTING**

---

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. It's not an IRS system.

---

## **K. SBU Data Use**

---

25. Does this system use, or plan to use SBU Data in Testing? No

---

## **L. NUMBER AND CATEGORY OF PII RECORDS**

---

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

26a. IRS Employees: Not Applicable

26b. Contractors: Not Applicable

26c. Members of the Public: Under 100,000

26d. Other: No

---

## **M. CIVIL LIBERTIES**

---

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

---

## **N. ACCOUNTING OF DISCLOSURES**

---



30. 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

---

**End of Report**

---