A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: January 8, 2016 PIA ID Number: **518**

1. What type of system is this? New

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

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

IRS Direct Pay, IRS Direct Pay

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:	Over 1,000,000

4. Responsible Parties: N/A

5. General Business Purpose of System

The IRS worked with Treasury Fiscal Service to develop a new online payment option for individual taxpayers called IRS Direct Pay that launched during the fourth quarter of 2013. IRS Direct Pay is a key initiative to help to drive individual adoption of electronic payments, which is a strategic priority for the IRS and Treasury. Each paper payment costs an average of $0.66 more per transaction to process than an electronic payment, so converting each additional 10% of individual taxpayers to paying electronically will save the IRS approximately $6.3 million per year in processing costs, and ensure that funds reach Treasury more quickly.

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*) No

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-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

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:

Taxpayers/Public/Tax Systems	Yes	
Employees/Personnel/HR Systems	No	
		Other Source:
Other	No	

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:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	No	No	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

10a. What is the business purpose for collecting and using the SSN ?

The SSN is collected to verify taxpayer identity to allow them to utilize Direct Pay and allow us to know where to post their payment.

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.)

A SSN must be collected in order to process payments.

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

SSNs will be masked upon entry. Currently any display of the SSN beyond entry displays only the last 4 digits of the taxpayers SSN. A future release of Direct Pay will remove SSNs from all screens apart from the ones where they are entered.

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

There is no way to eliminate the use of SSNs as long as they are what's used by the IRS to locate a taxpayer's account.

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.

Data Elements and Fields Collected: Tax Year Filing Status First Name Last Name Social Security Number Date of Birth Country Street Address Apartment Number PO Box City State Zip/Postal Code Information can be researched if there are any payment issues.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? No

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: No
b. Other federal agency or agencies: No
c. State and local agency or agencies: No
d. Third party sources: No
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.

PII collection is essential for this tool to allow the process and ability to properly apply payments.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	Yes	
To provide taxpayer services	Yes	
To collect demographic data	No	
For employee purposes	No	
		If other, what is the use?
Other:	No	

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:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)	Yes	Treasury Fiscal Service	Yes
State and local agency (-ies)	No		
Third party sources	Yes	First Data Corporation	Yes
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:

	YES/NO	**AUTHORITY**
Persistent Cookies	No	
Web Beacons	No	
Session Cookies	No	
		If other, specify:
Other:	Yes	Google Analytics

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?

Disclosure Agreement, Privacy Act, and Paperwork Reduction Act Authorization

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”?

The IRS Direct Pay Privacy notice (https://directpay.irs.gov/directpay/privacyNotice) contains verbiage that identifies due process when applicable. Due process is provided pursuant to 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

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

ID	Form Number	Form Name
2071	1545-0074	1040

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: Contractor Owned and Operated

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

	Yes/No	Access Level
IRS Employees:	No	
Users		
Managers		
System Administrators		
Developers		
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

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

Access to taxpayer data is determined by job function. Access to data is documented online in the security request application – Security Multi-User Request Forum (SMURF). An appropriate access level for each job function is also documented on the application security matrix document. Access is always granted on a “need-to-know” basis only.

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

Information entered for identity proofing is checked against IRS data through RPR-IUS (an IRS Web Service).

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.

At the end of the seven (7) year retention period, the media that contain the data are degaussed and then destroyed. A control log is maintained containing the media label Id, date and method of destruction, and the signature of the person who destroyed the media. This is in compliance with IRMs 1.15.32 and 25.10 for record retention and destruction.

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

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

NA

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. NA

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? No

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, SSN, to Name Photograph, IP Address) No

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