

Date of Approval: **November 13, 2019**

PIA ID Number: **4406**

## **SYSTEM DESCRIPTION**

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

View Debit, View Debit

*Is this a new system?*

Yes

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

SBSE Governance Board

*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.*

View Debit automates allowing qualified callers to hear a verbal review of an individual filer's master file account. On demand, processes requests sent by the Voice Response System (VRS) to query Integrated Data Retrieval System (IDRS) to determine if the taxpayer is eligible to receive account information via the automated system. If the taxpayer is not eligible, a route code defining the reason for denial will be sent. If eligible, the function will return to the VRS information on the tax modules available and whether or not each module has a balance due.

## 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

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

View Debit requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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

The Office of Management and Budget Circular A-130 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. View Debit requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer at this time.

*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

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?*

Yes

*Describe the other types of SBU/PII that are applicable to this system.*

Federal Tax Information

*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 items above are collected from the taxpayer to authenticate them prior to providing them with tax related information. This information represents the least amount of data needed to authenticate the individual, identify possible ID theft without any more information on user as possible using existing IRS command codes.

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

Accuracy: Authentication must include data in a prescribed format and must meet a variety of validation criteria that ensure proper validation to the appropriate account. Taxpayers are authenticated to check payments status on the IRS's Master Files before status information is returned to them. The app simply takes the SSN entered by the taxpayer and checks for it in the database; if it is found, they are required to enter a PIN which is then checked against the PIN connected to that SSN. If it's a match, they are granted access to that account's data.  
Timeliness: The system notifies the taxpayer with the date a payment has been received.

## **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 34.037 Audit Trail and Security Records

## 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

System Name: Modernized E-File (MeF)

Current PCLIA: Yes

Approval Date: 2/20/2019

SA&A: Yes

ATO/IATO Date: 2/9/2019

System Name: Security and Communications System (SACS)

Current PCLIA: Yes

Approval Date: 9/15/2018

SA&A: Yes

ATO/IATO Date: 11/5/2018

*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: 1040 Form Name: Individual Income Tax Return

*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?*

Yes

*Was an electronic risk assessment (e-RA) conducted on the system/application?*

Not Applicable

## 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 within View Debit comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. View Credit does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided via the IRS systems and their related 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):*

The information within View Debit comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. View Debit does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC. Published System of Records Notice in the Federal Register. The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for". Their response is mandatory under these sections. The taxpayers failing to provide the required information renders them ineligible to use the system.

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

The information within View Debit edit comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. View Credit does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided via the IRS systems and their related 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*

System Administrators: Read Only

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

Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user to be added. They must submit the request via the Online 5081 process to request access to the System.

## 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.*

1040X master data file and associated records will be disposed of in accordance with Records Control Schedule (RSC) 29 for Tax Administration- Wage & Investment, Item 55-56. Recordkeeping copies of system data will be destroyed on or after January 16, 6 years after the end of the processing year (Job No. N1-058-95-001). The media that contain the data are degaussed and then destroyed. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. 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.



## **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?*

5/29/2019

*Describe the system's audit trail.*

View Debit uses the Integrated Customer Communication Environment (ICCE) capability to capture audit data and forward the data to an Enterprise Logging System - Security Audit and Analysis System (SAAS). ICCE does not store audit data. Instead, audit records are created in memory and sent to SAAS as "forward and forget". There is no ability to access the audit information from the application or from the server on which the application runs.

## **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 DocIt (web-based document management system), an online secure repository.

*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?*

View Debit is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (now called Annual Security Control Assessment) occurs annually to ensure that controls remain in place to properly safeguard PII.

## **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: 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