Date of Approval: March 28, 2017 PIA ID Number: **2283**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. PDC-Pioneer Credit Recovery Inc., PDC-PCR

2. Is this a new system? Yes

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

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
Yes	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 primary business of Pioneer Credit Recovery Inc. is debt recovery. They contact borrowers and collect on defaulted tax amounts. A Private Debt Collector, Pioneer Credit Recovery Inc. (PDC-PCR) provides a portfolio of debt collection functions to support debt collection operations. This system includes both debt collections and debt accounting. PDC-PCR is a general purpose, multi-user system used throughout their locations. It provides electronic services such as: Debt Collection, Debt Accounting, Electronic forms, Databases, Call recording services and letter processing services (through third party- Taylor Communications)

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 No On Dependent

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

Yes	Social Security Number (SSN)

Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
Yes	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	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).

Per OMB-M-07-16 "mitigation strategy is currently not required. PDC-requires the use of Social Security Number's (SSN) because no other identifier can be used to uniquely identify the taxpayer. SSN's 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.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	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
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	No

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

Selected	SBU Name	SBU Description
Yes	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.
Yes	Proprietary data	Business information that does not belong to the IRS
No	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.

Pioneer uses the SBU/PII information received from the IRS, together with additional PII information received from the taxpayer and other third parties during the ordinary course of Pioneer's collections activities, in order to contact the taxpayer and increase the recovery of IRS tax debts and resolve IRS tax receivables by collection or other case resolutions. Pioneer only collects that PII (including SSN, which is used by the IRS and/or other third parties to assist in uniquely identifying a taxpayer) which is necessary for those purposes.

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

The DM9 collections system used by Pioneer is designed with logic checks to ensure data accuracy and integrity. Data from third party skip trace vendors is used to verify and enrich the client's data. Databases are updated and validated and are redundant allowing for the availability of the information. The security controls for the database is constantly reviewed to ensure safeguards are in place to protect the data.

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

SORNS Number	SORNS Name
Treas/IRS 26.019	Taxpayer Delinquent Accounts Files
Treasury/IRS 34.037	IRS Audit Trail and Security Records System

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? Yes

If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Private Debt Collection Data Transfer Component	Yes	01/27/2017	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).

Organization Name	Transmission method	ISA/MOU
U.S. Department of Defense (Defense Manpower Data Center (DMDC)	Electronic	No

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

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
IT Contractor	Vendor uses VMWare client to securely access VDI. Vendor must use RSA token for access and RDP to the respected servers.	No
Letter Vendor	Fed PII hits NESTfrom source system and is then encrypted with data encryption (PGP) and Secure FTP'd (SFTP)	No
Skip Trace Vendor	Part of the Waterfall process. File is sent via SSL to NEST from source system - then the file is encrypted with PGP and SFTP'd (SFTP) to SkipTrace Vendor's server.	No
Skip Trace Vendor	Part of the Waterfall process. File is sent via SSL to NEST from source system - then the file is encrypted with PGP and SFTP'd (SFTP) to SkipTrace Vendor's server	No
Skip Trace Vendor	Part of the Waterfall process; uses two different products, at different stages of the Waterfall process. File is sent via SSL to NEST from source system and is then encrypted with data encryption (PGP) and SFTP to the Skip Trace Vendor	No

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

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? Yes

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

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Private Debt Collection Data Transfer Component	Yes	01/31/2017	No	

Identify the authority and for what purpose? Federal legislation titled Fixing America's Surface Transportation (FAST) Act was enacted in December 2015 and requires the U.S. Department of

the Treasury, Internal Revenue Service (IRS) to proceed with a Private Debt Collection initiative. The IRS intends to implement this initiative in a phased approach beginning in Fiscal Year 2017. Pursuant to section 6103(h)(1) of the Internal Revenue Code (IRC). IRC 6103(h)(1) provides for disclosure of returns and return information to officers and employees of the Department of the Treasury (including IRS) whose official duties require access for tax administration.

12b . Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. Does this system disseminate SBU/PII to other Sources? Yes

If **yes**, identify the other source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Skip Trace Vendor	Subscription Service	No
Telephony System Vendor	Data logs- with supervision	No
IT System Vendor	Screen share	No
Letter Vendor	Electronic	No
IT Contractor	Screen share	No
Skip Trace Vendor	Subscription Service	No
Skip Trace Vendor	Subscription Service	No

Identify the authority and for what purpose? Skip Trace service; IT support service

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, cloud, 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?
By letter CP40 from the IRS; Notice is provided to individuals by other IRS applications or through forms (e.g, 1040 forms) that interact directly with the taxpayer at the time of collection. Due Process is provided pursuant to 5 USC. Also IRS sends Notice CP40 to the taxpayer advising that their case is being worked by a Private Collection Agency (Pioneer) and they may be contacted directly by that agency.

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):
Consent is implied, If a Tp does not want to use the PDC they can inform the IRS or PCA directly and the case will be recalled.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The entire Pioneer- Private Collection Agency process and procedures are dictated by the Internal Revenue Service and outlined in the Private Collection Agency Policy and Procedures guide. This guide directs the Private Collection Agency to allow the taxpayer due process to file a tax return, the right to opt-out of working with the Private Collection Agency, directs the Private Collection Agency to offer the taxpayer right to appeal, offers guidance to accept disputes to allow appropriate determinations to be made and covers privacy and policy statements to ensure due process for the taxpayer.

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)

Contractor Owned and Operated

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

IRS Employees? Yes

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

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read and Write	Moderate
Contractor Managers	Yes	Read and Write	Moderate
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	Yes	Read and Write	Moderate

21a. How is access to SBU/PII determined and by whom? System access is governed by roles and privileges using the 'least privilege' concept with the requisite approvals, reviews, and separation of duties. Use of the system data (with regard to who sees what data and what external vendors are approved to receive data) is covered in the Operational Plan.

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 ? No

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.

Information ages off (is deleted from) the system at varying intervals. All records housed in the PDC 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) 28 for Tax Administration-Collection, PART VII - PRIVATE DEBT COLLECTION (PDC) PROGRAM RECORDS; and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. Records Information & Management Office will perform a site visit at a later date.

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. The DM9 system is capable of auditing the following events: Any action that affects, modifies or changes the security settings of the system, functions of an application program; Security-related administration activity and security functions that affect user profiles or user access privileges; Changes that are made to selected and designated applications, programs and database tables; Clearing of the audit log file; Startup and shutdown of audit functions; Changes made to an application or database by a batch file; All system and data interactions concerning FTI. The DM9 system provides audit record generation capability for the auditable events listed above, allows the IT System Owner to select which auditable events are to be audited by specific components of the information system, and generates audit records for the events and with the content defined within our internal policies and standards. Audit logs for the following events are created and reviewed daily: log onto system, log off of system, creation or modification of super user groups, use or attempted usage of privileged access, sub-set of security administrator commands, while logged on in the security administrator role, sub-set of system administrator commands, while logged on in the user role, changes made to an application or database by a batch file, application critical record changes, changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility) and all system and data interactions concerning Taxpayer Data. Automated mechanisms, such as defined criteria reporting and our security information and event manager tool are used to monitor security events for suspicious behavior. Monitoring of activity is increased as necessary or if there is an indication of increased risk.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 2/28/2017

24.3 If **completed/ or in process,** 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?
In process and will include all applicable privacy requirements laid out by Publication 4812, working with Contractor Security Assessment Team to establish.

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: Under 5,000
26c. Members of the Public: 100,000 to 1,000,000
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? Yes

If **yes** , does the system have a process in place to account for such disclosures in compliance with IRC 6103 (p) (3) (A) or Subsection (c) of the Privacy Act? Contact *Disclosure* to determine if an accounting is required. Not Applicable

30b. If **N/A**, explain the Exemption and/or Disclosure s response. Per IRC §6103(k)(6) investigative disclosures are exempt from accounting requirements as defined in IRC §6103(p)(3)(A).

End of Report