Date of Approval: April 15, 2017 PIA ID Number: **2243**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Pindrop - Technical Demonstration, Pindrop

2. Is this a new system? Yes

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

Yes	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	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.

Pindrop Security's Fraud Detection System™ (FDS) identifies call spoofing, and other attempts to defraud organizations, by providing a highly accurate call risk score. It verifies caller location and caller device type and matches it against Caller ID or Automatic Number Identification (ANI) data to identify spoofing. Additionally, FDS leverages voice biometric capabilities, which combine caller voice data with calling device data, to create a unique Fraudster Profile that can be used to repeatedly, and accurately, identify a fraudster. Benefits - Identifies potential weaknesses in phone channel and how PII is disclosed. If a demonstrable problem is identified, IRS can take the necessary actions to provide a more secure environment of taxpayer data. How it will be used - It will be used as a tool to ensure fraud access to taxpayer data is blocked and warning notifications to IRS phone employees.

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)
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).

None - This information may or may not be collected in the recording of a telephone call. It is not data that is used for the technical demonstration. This is inherent information that is captured during the capture of key metrics of the call (ANI, GEO location, etc.)

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.

On Primary	On Spouse	On Dependent	Selected	PII Element
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
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	Yes	Yes

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

.

6d. Are there other types of SBU/PII used in the system? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. Call metadata; ANI (Caller ID/Phone), GEO location of caller, IRS employee Standard Employee Identification (SEID). Metadata is the supporting details of callers to the IRS: phone provider, network, mobile/landline, etc.

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

No	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 model creation and tuning process relies on call metadata (ANI/CLID=calling line identification) and Phone Reputation Service (PRS) query results to identify calling device type and relative geography of the calling device. Audio engineers will listen to calls of interest and produce sets of call recordings that will need to be analyzed by the IRS fraud analyst staff. Pindrop Security will then provide to the customer, weekly throughout the POC, batches of call audio to be evaluated for fraud. Pindrop Security is looking for the IRS to evaluate whether the call identified is “fraud”. Listening for: Voice Distortion – A technique used by fraudsters to artificially distort their voices to hide their identity. Caller voices may sound robotic, noisy, or “chipmunk-like”. Voice Disguising – A technique used by fraudsters to mimic female or male voices using falsetto or deep voice to match the gender of the actual account holder. Age Mismatch – A caller’s voice may not match the age of the actual account holder. Voice Mismatch – Listening to associated calls may indicate that suspected fraud calls do not sound like the normal voice of the actual account holder. Common Fraud Activities like SSN probing; Reconnaissance Suspect calls could be confirmed fraud event or suspect social engineering attempt, or “genuine”, meaning that the caller is indeed the identified caller and no suspicious activity is determined to have taken place. SSNs are not used, however due to the requirements of listening to call content the SSNs are overheard. If a call is flagged as potential fraud, then IRS analysts may perform further investigations to identify if taxpayer has experienced ID Theft, etc. Pindrop engineers will not have access to these IRS systems for research.

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

In the course of the Proof of Concept (POC), IRS fraud analyst(s) will be tasked with evaluation of batches of suspicious calls or other calls of interest to the POC. Investigation of a suspicious telephone call involves call listening mode, which involves the fraud analyst (IRS) listening to the suspect call (and any related calls) for any of the following threat indicators: Account reviewing involves looking up the account details of the associated call of interest to validate if any historical fraudulent activity has taken place on the account. If the call has a related account, review activity on the account for suspicious activity: new accounts, unusual transaction amounts or patterns, reported fraud, or evidence of risky transactions

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? No

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 PCLIA	Approval Date	SA&A?	Authorization Date
Verint/Vovici	Yes	08/28/2015	No	

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agencies? No

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

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

If **yes**, identify the forms
No Tax Form Records found.

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

If **yes**, identify the forms
No Employee Form Records found.

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

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.? Yes

14a. If **yes**, briefly explain how the system uses the referenced technology. Virtual Private Network connected to Pindrop (from IRS) to analyze call metadata; GEO location comes into play and the ANI. Results are sent back to resident Pindrop hardware at IRS.

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? No

17b. If **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.
Follows Contact Recording protocol. "Contact Recording" is a telephone application/tool/system that records incoming "toll-free" telephone contacts for the purpose of possible subsequent monitoring. Incoming calls are answered with an additional announcement that states, "Your call may be monitored or recorded for quality purposes." The system has been implemented in all Accounts Management and Compliance Services call sites. Managers and Quality Review use the tool to perform required random reviews (performance and product) of incoming telephone contacts. While the system provides screen capture of account actions, as well as voice recording of the call, the recordings are NOT accessible by TIN, voice processing personal identification number, PIN, or any other TIN. The system stores data by employees SEIDs for a maximum of 45 days.

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):
They can request not to be recorded, IRS stops the action. Therefore, anyone requesting not to be recorded would not be part of the sample we wish to capture for this POC.

19. How does the system or business process ensure due process regarding information access, correction and redress? Follows Contact Recording protocol as listed in 17b.

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? No

Contractor Employees? Yes

Contractor Employees	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	No		
Contractor Sys. Admin.	No		
Contractor Developers	No		

21a. How is access to SBU/PII determined and by whom? Pindrop audio engineers will listen to calls of interest (below) and produce sets of call recordings that will need to be analyzed by IRS fraud analyst staff. At this point of listening the audio engineers will hear the conversation between the taxpayer and the IRS phone representative. Although the intent is not to gather the PII, the process of identifying potential fraud inadvertently allows the PII to be heard. Pindrop Security will then provide to the customer, weekly throughout the POC, batches of call audio to be evaluated for fraud. Calls of interest: After audio and metadata had been loaded and validated, the Pindrop Security audio engineers will begin analyzing the data. Audio engineers will examine PRS data in conjunction with creating audio models that will be used to identify the fraudulent phone calls. The model creation and tuning process relies on call metadata ANI/CLID and PRS query results to identify calling device type and relative geography of the calling device. The PRS information is used to identify anomalies in the call data sets where there is a discrepancy between the phone carrier data and FDS detected device type and geolocation. Customer-provided representative fraud and confirmed fraud calls are Phoneprinted™ and voiceprinted and a fraudster profile is created. This fraudster profile is then used to identify repeat callers (specifically calling devices and fraudster voices) regardless of the ANI/CLID presented or voice of the caller.

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.

After the POC conclusion (8 weeks), and final presentations, a Pindrop Security engineer will wipe all data on the POC appliances and Pindrop-provided workstation(s) before they are returned to Pindrop, using a certified data erasure tool. The typical method employed by

Pindrop uses a Department of Defense 5220.22-M 3- pass wipe, which overwrites the data on the disk in three passes. At the completion of the wipe, a certificate of destruction will be generated and provided to the customer. Pindrop is sensitive to customer data security requirements and will accommodate most additional data handling and destruction requests. If a customer's requirement for data destruction specifies physical destruction of magnetic media (degaussing or crushing) or that the customer should retain the magnetic media at the end of the POC, it should be noted in the POC Statement of Work. All records housed in the Pindrop System will be erased or purged from the system in accordance with approved retention periods. It is not the official repository for data and documents and does not require National Archives approval to affect data disposition. Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS General Records Schedules 3.2 for Information System Security Records, and as coordinated with the IRS Records and Information Management 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. The POC demonstration utilizes controlled call recordings with no access to IRS production networks. The demonstrator uses Caller ID phone data to perform analysis and flags potential calls as fraudulent, IRS phone fraud team would review calls to substantiate potential fraud. The demonstrator would have no access to IRS/taxpayer systems which would generate audit trail criteria.

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? 07/15/2017

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?
Connectivity testing between archived Contact Recording calls and POC Pindrop hardware. Pindrop is responsible for developing and hosting the application per a Memo of Understanding (MOU) with the IRS. The MOU includes all the applicable disclosure, retention, safeguards and confidentiality clauses as reviewed and approved by the Offices of Disclosure and Procurement. There is a standard User Acceptance Testing plan that is updated as needed based on the changes requested in order to appropriately address privacy requirements. Test plan date above is subjective to approvals of demonstration. Total POC is slated for 8 weeks, date above is a placeholder.

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: 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? No

End of Report