Date of Approval: February 8, 2017 PIA ID Number: **2021**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Criminal Investigations Refund Fraud and Crimes Prevention Support Services, C4S

2. Is this a new system? No

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

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

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

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

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
No	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.

Criminal Investigations has obtained a contractor provided service, to enhance their ability to monitor and detect criminal actors on the deep and dark web who are engaged in tax and other financial fraud. The service delivers customized collection and analysis of activity on the dark web

related to tax fraud and other crimes. When relevant information is found by the provided service it is delivered to CI through a series of intelligence reports. The information is used by CI to generate leads for new investigations as well as to support ongoing criminal investigations that touch the dark web. Where possible, data recovered from the dark web is shared with other IRS stakeholders to mitigate potential harm to taxpayers who could be victims of identity theft.

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)
No	Individual Taxpayer Identification Number (ITIN)
No	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).

The information this system would collect is stolen or otherwise compromised PII that is posted both publicly or in closed forums on the dark web. The contracting analysts will be monitoring for the compromised PII and informing IRS-CI of the location of the information. The system uses the full SSN and a mitigation strategy is currently not required. No alternative exists currently for the application. This program is aware of and part of the IRS-wide SSN elimination and reduction program

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	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	Place of Birth	No	No	No
No	SEID	No	No	No
Yes	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
Yes	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
Yes	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? Yes

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

Selected	SBU Name	SBU Description
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
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
Yes	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)
No	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
Yes	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 provided service is engaged in monitoring the dark web for PII that is posted both publicly and in closed forums. The PII is often stolen or otherwise compromised data from other public and private entities that is offered for sale by bad actors on the internet. The Contracting analysts will find the stolen PII and inform IRS-CI of the location of the compromised PII through a series of intelligence reports. These intelligence reports are critical information to help IRS-CI in initiating new investigations as well as supporting ongoing criminal investigations. If stolen PII is recovered, IRS-CI will share the recovered data with other IRS stakeholders to help protect taxpayer IRS accounts. IRS-CI may also provide the Contracting analysts with SBU data that is related to ongoing investigations. The SBU data would primarily include online monikers of bad actors, but could also include names or account numbers of individuals under criminal investigation, or who are otherwise related to ongoing criminal investigations. This information would be used by the Contracting analysts to assist in searching the dark web for any activity related to these individuals or online monikers.

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

IRS-CI is committed to ensuring that its law enforcement practices concerning the collection or retention of data are lawful and respect the important privacy interests of individuals. As part of this commitment, IRS-CI operates in accordance with rules, policies and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of the provided service. It should be noted that IRS-CI does work closely with other federal, state and local law enforcement partners and provides technological assistance under a variety of circumstances, such as in joint federal grand jury investigations. IRS-CI's policy ensures individual right's are not violated, as all data collection activity will be supervised by IRS-CI and will be gathered pursuant to existing authorities already granted to IRS-CI.

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

IRS 46.005	Electronic Surveillance and Monitoring Records

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? 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
Internet Forums which are not controlled by IRS	Online	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? 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, 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? 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.
The PII that would be discovered by the provided service would have been posted online by a bad actor and therefore is only available from third party sources.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? The PII that would be discovered by the provided service would have been stolen or otherwise compromised PII posted online by a bad actor and therefore prior consent is not possible.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Any collection of data that was posted online by a bad actor would be gathered pursuant to existing authorities granted IRS-CI to collect evidence in a criminal investigation. All evidence gathered would be protected under existing IRS-CI authority.

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	No	
Sys. Administrators	No	
Developers	No	

Contractor Employees? Yes

Contractor Employees?	**Yes/No**	**Access Level**	**Background Invest. Level**
Contractor Users	Yes	Administrator	High
Contractor Managers	Yes	Administrator	High
Contractor Sys. Admin.	No		
Contractor Developers	Yes	Administrator	High

21a. How is access to SBU/PII determined and by whom? Stolen or otherwise compromised PII will be discovered online by the Contracting analysts who will alert IRS-CI of it's existence through a series of intelligence reports. SBU data will be provided by IRS-CI to the

Contracting analysts to assist them in searching the dark web for information to support existing IRS-CI criminal investigations.

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.

The contractor is the owner of the records and the IRS is not able to dictate record retention policies. Any records generated and maintained from 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) 30, Item 15 for Investigative Files and Related Records, 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? Do not know

23.1 Describe in detail the system s audit trail. We don't keep the audit trail, as the system belongs to the contractor. Only the relevant information is provided to the IRS?

J. PRIVACY TESTING

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

24c. If **no**, please explain why. IRS does not own the system.

K. SBU Data Use

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

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

If **yes,** provide the date the permission was granted.

If **no**, explain why not.

25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments?
If **no**, explain why not.

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? Yes

If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring. The provided service will be monitoring the dark web and criminal forums for information that is offered for sale by bad actors that could be used in tax or other financial fraud. The monitoring will be conducted under supervision of IRS-CI and will be done pursuant to existing IRS-CI authorities and policies.

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

End of Report