Date of Approval: August 1, 2017 PIA ID Number: **2672**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Criminal Investigation Electronic Crimes Environment, CI2/ECE

2. Is this a new system? No

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

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

CI2/ECE 1950

Next, enter the **date** of the most recent PIA. 11/21/2016

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
Yes	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

Were there other system changes not listed above? Yes

If yes, explain what changes were made. The ECE system is moving its block level San storage to the IRS CI Enterprise Storage Service (ESS) located in the Secured caged CI space in the Memphis, Tenn., Enterprise Computing Center of which only CI personnel can access un-escorted. CI1 GSS storage admins and CI2/ECE GSS storage admins will administer all connected switches accessing the San Block storage service and manage all volumes and storage containers. The CI ESS system is to go online June 6, 2017. CI ESS is also going online at the Martinsburg, W. Va. Enterprise Computing center which differs from the MEM ECC in that it does not have caged system space specific to CI. CI's systems are grouped together in one area of the data center and locked with CI cabinet locks, systems are also monitored 24/7 by security cameras and local security staff (It is a level 5 facility).

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? Yes

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.

Electronic Crimes Technology Support Center (ECTSC) Criminal Investigation Workgroup Criminal Investigations (CI-2) provides the information technology infrastructure that supports the Criminal Investigation (CI) core mission of serving the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law. The Electronic Crimes Environment (ECE) application resides on CI-2 and provides the necessary tools to securely access and collaborate on electronic case evidence.

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).

There is no plan to remove SSN's from cases since agents work with other Federal Agencies to prosecution of cases. The Office of Management and Budget memorandum M-17-12 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. Criminal

Investigation Electronic Crimes Environment requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs 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	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
Yes	SEID	No	No	No
Yes	Mother's Maiden Name	No	No	No
Yes	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	Internet Protocol Address (IP Address)	No	No	No
Yes	Criminal History	No	No	No
Yes	Medical Information	No	No	No
Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
Yes	Passport Number	No	No	No
Yes	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
Yes	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.
Yes	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
Yes	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? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. Subpoenaed Digital evidence may contain any information about subjects, their contacts, companies, criminal organizations and enterprises. Federal and other law enforcement agent information can also be included with the evidence.

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
Yes	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
Yes	PII for personnel administration is 5 USC
Yes	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.

IRS Criminal Investigations' Electronic Crimes performs federal law enforcement search warrant acquisitions to preserve, store, analyze, and process digital evidence in a forensically sound manner to support criminal investigations. Digital evidence is seized read only in its entirety and cannot be changed. During processing and analysis, the evidence matching the scope of the warrant is extracted from the forensic image and presented to the case agents for review. CI2/ECE

is one of the Electronic Crimes' tools for performing these operations. PII, SBU and SSN's may or may not be in the seized digital evidence which we do not control and CI2/ECE case metadata for case management uses agents SEID and Case numbers. All cases in CI2/ECE have independent locked down virtual infrastructure and access lists based on court approved assigned agents. There is no interaction or ability to search across or combine information and evidence between cases. To effectively preserve, store, analyze, and process seized data in a forensically sound manner to support criminal investigations. Provide users (Special Agents) with the necessary infrastructure to securely access and collaborate on seized evidentiary case data. Ensure that seized digital evidence is expeditiously and securely accessible. Agency is enforcing tax laws. SSNs are required for cases that point to an individual and are unique to the individual. There is no mitigation strategy. CI Ecrimes cannot control the information in the seized/subpoenaed evidentiary data and we cannot change it, we can only control the access to it. The data may contain anything. All elements should be selected but the evidence may contain only a couple elements or none at all.

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

Investigative Purposes require that these data elements be collected to support the investigation regardless of whether or not another source exists. Electronic Crimes' federal forensically trained law enforcement agents seize and forensically image the digital evidence it is read only and cannot be changed, all elements in the forensic images are verified with MD5 hashes which must not change or it will not be acceptable as evidence. If the evidence images contain PII, SBU, SSN, or other sensitive information it is maintained as part of the image and cannot be altered. Only the assigned case agents have access to the evidence through forensic tools in the CI2/ECE system. If any of this information is part of evidence in the scope of the warrant, then it will be presented in criminal trial proceedings un-altered.

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
RS 24.06	Customer Account Data Engine Business Master File
IRS 34.037	Audit Trail and Security Records System
IRS 46.009	Centralized Evaluation and Processing of Information
IRS 46.005	Electronic Surveillance Files
IRS 24.030	Individual Master File

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? 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
ICE	Electronic evidence. I/E Hard drives	No
FBI	Electronic evidence, I/E Hard drives	No
Secret Service	Electronic evidence, I/E Hard drives	No

11c. Does the system receive SBU/PII from State or local agency (-ies)? Yes

If **yes**, for each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agenc Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Secret Service	Case images, records, data sets or other electronic data	No
Immigration Customs Enforcement (ICE)	Case images, records, data sets or other electronic data	No
Postal	Case images, records, data sets or other electronic data	No
FBI	Case images, records, data sets or other electronic data	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
Dependent upon the case, CI-2 can receive data in the form of evidence or work products from other third party sources	The work product could be case images, records, data sets, or other electronic data related to a criminal investigation	No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
1040	Tax Form

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, 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?
Court ordered Subpoena, following the judicial processes for the federal district of the law enforcement action. IRS CI may or may not be the lead on the case judicial process, it could be other federal agencies with IRS CI Electronic Crimes the lead on the digital evidence review. In regards to any information retrieved off tax returns, the IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

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? Court ordered Subpoena requiring Law Enforcement actions. The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information

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

The system is designed to only allow Case defined agent access to the specific case evidence. System Administrators have no access to case data. Case data resides in specifically configured virtual machines on independent virtual networks with specifically defined local use accounts for the assigned case agent. The CI2/ECE system is a certified FISMA High security system which requires full auditing and tracking of user access through the systems and is tested and recertified every year on its security and auditing processes. The system does not replace any individual taxpayer's right to due process, as dictated by the Internal Revenue Manual guidelines. IRS policy allows individual taxpayers whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. However, due to the nature of this system, individuals may not receive specific notice that their information has been collected.

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)

IRS 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	Yes	Administrator
Developers	Yes	Administrator

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? Access to the Criminal Investigation Electronic Crimes Environment is requested via an Online (OL) Form 5081. Access is granted on a need-to-know basis. The OL5081 enrollment process requires that an authorized manager approve access requests on a case by case basis. Access approval is based on the Users role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments, they are restricted from changing the boundaries of their access without management approval. The

employee's access will be terminated once they no longer require access to the Database. Deletion from the active access role is also performed through the OL5081.

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? Yes

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.

IRM 1.15.30, which moved from IRM 1.15.30 and published as RCS 30 in Document 12990, Records Management, Records Control Schedule for Criminal Investigation - Administration Records. • Travel Vouchers – Destroy after one year. • Special Investigative Equipment Custody and Control Records, Forms 1930, Custody Receipt for Government Property- Destroy after 3 years. • Investigative Files – Retire to FRC 2 years after case is closed. Destroy after 10 years. • Collateral Investigation Reports- Destroy one year after closing. • Daily Diaries – Retire to FRC when 4 years old. Destroy after 10 years. All ECE data relating to a CI investigation will be removed/disposed of by the Lead Agent (CIS/Investigator) in accordance with Investigative Case Files under RCS 30, item 15

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)? Yes

23a. If **yes**, what date was it completed? 11/8/2016

23.1 Describe in detail the system s audit trail. System administrators maintain all data in folders that have specific rights granted to each user. Logs are created to track the files viewed by each user. These logs can be used to audit the data accessed by a given user as well as provide chain of custody documentation for the resource. Audit events captured by the system audit logs: Logon and logoff Password changes data object access such as open and closed. Reading, editing and deletion of object files. Date and time of event. The unique identifier (user name, SEID, application name, etc.) of the user or application initiating the event.

J. PRIVACY TESTING

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

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

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? Annual Security Control Assessment

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? TFIMS

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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:	Under 50,000
26b. Contractors:	Under 5,000
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? 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