Date of Approval: **June 08, 2020**

PIA ID Number: **5157**

SYSTEM DESCRIPTION

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

Electronic Crimes Environment, ECE

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

ECE, PIA # 2672

What is the approval date of the most recent PCLIA?

8/1/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

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

Criminal Investigation Governance Board (CIGB)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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.

The Electronic Crime's Environment (ECE) is an environment that can create virtual settings to handle the processing, analysis, storage, and archiving of seized digital evidence. It offers forensic and analytic capabilities to extract and document criminal activities from information obtained during the criminal case investigations. Electronic Crimes (EC) investigations involve digital and multimedia evidence of a variety of types and sources, such as, but not limited to: witnesses, subpoenas, personal computers, mobile devices (phones, tablets, etc.), small and large business computers/servers, server farms, cloud storage or the Dark net. ECE provides CI investigators with a digital evidence portal, accessible nationwide.

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:

Law enforcement and intelligence purposes

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

Used in Criminal Investigation to uncover potential criminal actions

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 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. 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.

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

Phone Numbers

E-mail Address

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

Mother's Maiden Name

Protection Personal Identification Numbers (IP PIN)

Internet Protocol Address (IP Address)

Criminal History

Medical Information

Certificate or License Numbers

Vehicle Identifiers

Passport Number

Alien Number

Financial Account Numbers

Photographic Identifiers

Biometric Identifiers

Employment Information

Tax Account Information

Centralized Authorization File (CAF)

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.

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

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

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.

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.

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

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

PII for personnel administration is 5 USC

PII about individuals for Bank Secrecy Act compliance 31 USC

Information by CI for certain money laundering cases may be 18 USC

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.

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. 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 ECE case metadata for case management uses agents SEID and Case numbers. All cases in 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.

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

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.

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 24.046 Customer Account Data Engine Business Master File

IRS 34.037 Audit Trail and Security Records

IRS 46.005 Electronic Surveillance and Monitoring Records

IRS 24.030 Customer Account Data Engine Individual Master File

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?

No

Does the system receive SBU/PII from other federal agency or agencies?

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).

Name: Immigration and Customs Enforcement
Transmission Method: Electronic evidence. I/E Hard drives
ISA/MOU: No

Name: Federal Bureau of Investigation
Transmission Method: Electronic evidence, I/E Hard drives
ISA/MOU: No

Name: Secret Service
Transmission Method: Electronic evidence, I/E Hard drives
ISA/MOU: No

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

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-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: ICE
Transmission Method: Case images, records, data sets or other electronic data
ISA/MOU No

Organization Name: Secret Service
Transmission Method: Case images, records, data sets or other electronic data
ISA/MOU No

Organization Name: Postal
Transmission Method: Case images, records, data sets or other electronic data
ISA/MOU No

Organization Name: FBI
Transmission Method: Case images, records, data sets or other electronic data
ISA/MOU No

Does the system receive SBU/PII from other sources?

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: Dependent upon the case, CI-2 can receive data in the form of evidence or work products from other third party sources
Transmission Method: The work product could be case images, records, data sets, or other electronic data related to a criminal investigation
ISA/MOU No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: Form 1040 Form Name: Tax Form

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?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

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.

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 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.

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 Contractor Operated

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

IRS Employees

Users: Read Only

System Administrators: Administrator

Developers: Administrator

IRS Contractor Employees

Contractor System Administrators: Administrator

Contractor Developers: Administrator

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.

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.

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 - GRS 1.1 Item 010/ Destroy 6 years after final payment or cancellation. Special Investigative Equipment Custody and Control Records, Forms 1930/ RCS 30 Item 11 Destroy 3 years after, 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

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?

11/8/2019

Describe 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.

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)?

Treasury FISMA Inventory Management System (TFIMS)

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?

Annual Security Control Assessment

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: Under 50,000

Contractors: Under 5,000

Members of the Public: Under 100,000

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?

Yes

Does your matching meet the Privacy Act definition of a matching program?

Yes

Can the business owner certify that it meets requirements of IRM 11.3.39, Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Yes

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