Date of Approval: **April 30, 2020**

PIA ID Number: **4732**

SYSTEM DESCRIPTION

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

Chief Counsel System Domain, CC-1

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?

Chief Counsel System Domain, CC-1, ID# 2177

What is the approval date of the most recent PCLIA?

2/9/2017

Changes that occurred to require this update:

Significant System Management Changes

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.

Infrastructure Executive Steering Committee (IESC)

Current ELC (Enterprise Life Cycle) Milestones:

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 Office of Chief Counsel (IRS) is staffed by roughly 2200 attorneys, assorted professionals, and administrative and clerical support personnel. This highly skilled workforce litigates thousands of cases annually in the US Tax Court, provides tax and general legal support and advice to the IRS, represents the IRS in bankruptcy proceedings, provides public and private guidance to taxpayers, and much more. The Chief Counsel System Domain (referred to as the CC-1 GSS) provides the Office of Chief Counsel the network infrastructure to accomplish its mission. The CC-1 GSS spans multiple sites. The infrastructure includes servers, workstations, printers etc. CC-1's servers host both Commercial Off The Shelf (COTS) and in-house developed applications. These applications track a vast legal workload and provide other necessary tools that keep the nation's largest single practice law firm functioning. Due process is provided outside of the system by applicable law.

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:

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

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

The IRS employs many attorneys that act on behalf of the IRS. They provide legal support and advice for the IRS such as negotiating tax treaties, handling legal cases (e.g. tax cases brought to the United States Tax Court), representing the IRS in bankruptcy proceedings, petitions, and more. Those attorneys, as well as support personnel (secretaries, paralegals, IS professionals, etc.) work within the Chief Counsel's office. The Chief Counsel System Domain (referred to as the CC-1 System) is responsible for providing the network infrastructure for those attorneys and support personnel.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

The system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system.

Employer Identification Number

Other Taxpayer Identification Number

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

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

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

Are there other types of SBU/PII used in the system?

No

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

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.

In cases where PII is being sent out of the agency, we encrypt our emails and sometimes attach encrypted zip files to emails when sending attachments. Additionally, any materials placed on hard drives, thumb drives, CDs and DVDs that may have PII enclosed are zipped in encrypted containers (256 bit encryption) using SecureZip or WinZip. Most transfers of files that contain PII would likely be with TIGTA, DOJ, Congress (tax writing committees) and outside experts. Productions to non-tax writing committees in Congress, the tax payers and their Counsel would be redacted for privilege and 6103 before leaving the agency. As for its disposal, that usually happens at the close of a case for most parties, though my group does not control that. Destruction of all evidence is sometimes ordered by the court or drawn up in settlements, closing agreements, etc. by the attorneys and it is up to the custodians of the produced files to follow through with it. Email messages exiting the CC-1 environment are scanned for numeric patterns that match that of an SSN. Encrypted content cannot be

scanned, due to the nature of the encryption, so those pass through. When we detect an unencrypted SSN egressing the CC-1 environment, we return a non-delivery report of the message to the sender and hold a copy on the scanning server for 15 days. Term Non-delivery Report (NDR) is basically an email response saying your email message was not delivered.

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

Information is provided by Federal Courts and IRS. Each data item is reviewed by Chief Counsel personnel for accuracy, timeliness and completeness.

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 34.037 Audit Trail and Security Records

IRS 36.003 General Personnel and Payroll Records

IRS 90.001 Chief Counsel Management Information System Records

IRS 90.002 Chief Counsel Litigation and Advice (Civil) Records

IRS 90.003 Chief Counsel Litigation and Advice (Criminal) Records

IRS 90.004 Chief Counsel Legal Processing Division Records

IRS 90.005 Chief Counsel Library Records

IRS 90.006 Chief Counsel Human Resources and Administrative Records

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?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: CASE-TLCATS
Current PCLIA: Yes
Approval Date: 5/9/2019
SA&A: Yes
ATO/IATO Date: 8/8/2019

System Name: CASE-MIS
Current PCLIA: Yes
Approval Date: 3/14/2018
SA&A: Yes
ATO/IATO Date: 1/12/2020

Identify the authority

http://www.irs.gov/pub/irs-wd/00-0075.pdf http://www.law.cornell.edu/uscode/text/26/6109 Section 7801 and 7803 of the Internal Revenue Code.

For what purpose?

http://www.irs.gov/pub/irs-wd/00-0075.pdf http://www.law.cornell.edu/uscode/text/26/6109 Section 7801 and 7803 of the Internal Revenue Code.

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: Department of Justice
Transmission Method: Electronic Discovery
ISA/MOU Yes

Organization Name: Tax Courts
Transmission Method: Electronic Discovery
ISA/MOU Yes

Identify the authority

http://www.irs.gov/pub/irs-wd/00-0075.pdf http://www.law.cornell.edu/uscode/text/26/6109 Section 7801 and 7803 of the Internal Revenue Code.

Identify the Routine Use in the applicable SORN (or Privacy Act exception)

N/A

For what purpose?

http://www.irs.gov/pub/irs-wd/00-0075.pdf http://www.law.cornell.edu/uscode/text/26/6109 Section 7801 and 7803 of the Internal Revenue Code.

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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?

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.

Not applicable - CC-1 does not collect any PII on individuals but tracks case calendars and workload schedules through CASE-MIS. CASE-MIS has a separate PCLIA on file.

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

No

Why not?

Not applicable - CC-1 does not collect any PII on individuals but tracks case calendars and workload schedules through CASE-MIS. CASE-MIS has a separate PCLIA on file.

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

Not applicable - CC-1 does not collect any PII on individuals but tracks case calendars and workload schedules through CASE-MIS. CASE-MIS has a separate PCLIA on file.

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 Operated

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

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Administrator

Developers: Administrator

IRS Contractor Employees

Contractor Developers: Administrator

How is access to SBU/PII determined and by whom?

User access requests are authorized by Chief Counsel management and by a select set of management analysts in the Office of Chief Counsel. Access requests are authorized using the Online 5081 (OL5081) system. These management analysts determine the level of access granted each user by the application. A user's access to the data terminates when it is no longer required. User's access is terminated by a system administrator upon a manager request or upon automatic account removal notice received from OL5081 system of user employment termination. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on Form 5081.

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.

For different data types, there are different retention periods. Retention schedules are documented in the Functional specification packages. All CC-1 records are scheduled, and maintained in accordance with IRS Document 12990, Records Control Schedule Chapters 13 and 14. All data meeting end of retention period requirements will be eliminated, overwritten, degaussed, and/or destroyed in accordance with National Archives and Records Administration (NARA)-approved disposition authorities for that system's data, and done so in the most appropriate method based upon the type of storage media used. The method used for sanitization will follow NIST SP 800-88 guidelines. GRS 3.2 Item 060/61-PKI administrative records. -Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.

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?

3/31/2017

Describe the system's audit trail.

CC-1 relies on audit trails via Windows.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

System Development works with Quality Assurance to perform testing (Unit, System Acceptance Testing (SAT), Integration, Regression and User Acceptance). They also work with Quality Assurance with regard to updates for existing applications including security and role-based access restrictions. The WPC is run monthly on all Windows servers where these applications are installed and used. Specific unit testing occurs for all new source code, as well as negative and role-based testing over security to ensure security posture is maintained. New security flaws result in a new problem ticket and existing flaws that are not remediated continue to be tracked to resolution.

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: Not Applicable

Contractors: Not Applicable

Members of the Public: 100,000 to 1,000,000

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?

No

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