Date of Approval: **March 13, 2019**

PIA ID Number: **3889**

SYSTEM DESCRIPTION

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

Chief Counsel Advice Check System, CCACheck, Release 2.2, CCA Check

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 Advice Check System, CCACheck, Release 2.2, CCA Check, PIA # 1550

What is the approval date of the most recent PCLIA?

3/9/2016

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.

There is no formal governance board or ESC for this system.

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?

No

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 CCA Check System is a software application connected to the email program of the IRS Office of Chief Counsel designed to ensure that the IRS Office of Chief Counsel is complying with the obligation imposed by law to disclose to the public the legal advice contained in a specified category of email messages. It is the practice of the IRS Office of Chief Counsel not to retrieve the resulting records by any individual identifier.

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)

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

If an SSN is included in an email, that information is maintained in the system. The collection of the emails in the system is necessary to ensure that the IRS Office of Chief Counsel is complying with the obligation imposed by law to disclose to the public the legal advice contained in a specified category of email messages.

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

Mitigation is that (1) SSNs are rarely included in the original email message pursuant to the IRS Office of Chief Counsel's standards for using email; and (2) when an SSN is included in the original email message, the SSN is redacted prior to any public availability.

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

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

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

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

Procurement sensitive data Contract proposals, bids, etc.

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.

Proprietary data Business information that does not belong to the IRS

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

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities

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?

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

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.

The need and use for SBU/PII arises because CCA Check is an application employed to withhold such information from certain email communications prior to mandatory public disclosure. CCA Check neither uses nor generates SBU/PII (it stores information about withholding of such information from these email communications).

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

CCA Check does not verify the accuracy of information. It stores information about how SBU/PII was withheld from those emails.

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 90.002 Chief Counsel Litigation and Advice (Civil) Records

IRS 90.003 Chief Counsel Litigation and Advice (Criminal) 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?

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.

This is a process by law. Due process is provided via 5 USC.

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

No

Why not?

CCA Check process is mandated by law. Due process is provided via 5 USC.

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

There is no option to "search" or "correct". If the IRS fails to comply with the law regarding the withholding, there would be an opportunity for a civil lawsuit by a victim. Due process is provided via 5 USC.

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 Write

System Administrators: Read Write

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

SA (System Administrators) determine who is eligible to access the system according to their role. IRS employees request access by submitting an Online 5081 which must be approved by the SA.

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.

All records housed in the 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. The official record keeping system for Section 6110 Chief Counsel Advice is properly scheduled under Records Control Schedule (RCS) 14 for Associate Chief Counsel, Item 5, and housed for public inspection under the IRS Written Determination page on IRS.gov, as scheduled under Records Control Schedule (RCS) 17 for Information Technology, Item 25, 2(a).

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

In the current application database, audit trailing is implemented. IRM 10.8.1 require auditing processes on each table and event. This auditing will include capturing the following: insert date and time, inserted by, update date and time, updated by. The data that CCA Check receives is from internal IRS systems which are deemed reliable and the data is validated for accuracy by the system sending the data as described in that system's PCLIA. CCA Check is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

This is an internally created legacy software tool that did not follow an Information Technology (IT) path in development because it is defined as a tool/utility and not a separate system.

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?

Yes

Explain the First Amendment information being collected and how it is used.

If the issue is addressed in an email, that information is maintained in the system. The information in this system is not used to take action with respect to any person.

Please list all exceptions (any one of which allows the maintenance of such information) that apply:

The information maintained is pertinent to and within the scope of an authorized law enforcement activity (as noted in Q 7).

There is a statute that expressly authorizes its collection (identified in Q6).

Will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges under Federal programs?

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