

Date of Approval: March 9, 2016

PIA ID Number: **1550**

A. SYSTEM DESCRIPTION

1. 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

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.

PIA 930

Next, enter the **date** of the most recent PIA. 4/1/2015

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
Yes 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

Were there other system changes not listed above? No

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.

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 Office 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 Office not to retrieve the resulting records by any individual identifier.

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).

Mitigation is that 1) these numbers are rarely included in the original email message and 2) when they are included, they are redacted prior to any public availability.

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.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
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
No	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

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	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
Yes	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)

<u>Yes</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>Yes</u>	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.

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 the withholding of such information from these email communications}.

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

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

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? No

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. *Redacted information for Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? 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. This is a process by law. Due process is provided via 5 USC .

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

19. 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 civil lawsuit by a victim. Due process is provided via 5 USC .

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

<u>IRS Employees?</u>	Yes/No	Access Level(Read Only/Read Write/Administrator)
Users	Yes	Read-Only
Managers	Yes	Read and Write
Sys. Administrators	Yes	Read and Write
Developers	No	

Contractor Employees? No

21a. 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 OL5081 which must be approved by the SA.

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.

All records housed in the Chief Counsel Advice Check System (CCACheck) 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).

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? 6/29/2015

23.1 Describe in detail the system s audit trail. Middle Tiers: IRS Audit trail requirements are not implemented for these three systems. Database Tier: Database auditing is configured and audit records are captured for the following activities : use of database system privileges; statements which create, alter, delete, or rename database objects or users; session connections and failures including the usage of invalid passwords or user account, and the audit of privileged user (SYSDBA) operations. The audit trail is protected from unauthorized access. The system does not audit changes to application data including select, insert, update, or delete activities.

J. PRIVACY TESTING

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

24c. If **no**, please explain why. N/A

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: Not Applicable
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? Yes

27a. If **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 this system. The information is this system is not used to take action with respect to any person.

27b. If **yes**, please check all of the following exceptions (any one of which allows the maintenance of such information) that apply:

The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance (as noted in Q17). No
The information maintained is pertinent to and within the scope of an authorized law enforcement activity. (As noted in Q 7) Yes
There is a statute that expressly authorizes its collection. (Identified in Q6) Yes

27c. If **yes**, will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges? 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
