

**Department of the Treasury
BUREAU OF ENGRAVING AND PRINTING**

**Chief Counsel System
Matters Tracking System
(CCS-MTS)**



December 17, 2015

Privacy Impact Assessment (PIA)

A. Contact Information

System/Project Name	Chief Counsel System Matters Tracking System (CCS-MTS)
OMB Unique Identifier	Not Applicable; not a collection of information necessitating OMB unique identifier.
FIPSS 199 Category	Moderate

1. Who is the person completing this document?	
Name / Title	Scott Graf; Info Security Engineer
Office/Division	Office of Critical Infrastructure & Information Technology Security /Information Technology Audit & Compliance Division
Phone Number	(202)-874-3578
Email Address	Scott.Graf@bep.gov

2. Who is the system owner?	
Name / Title	Sidney Rocke, Chief Counsel
Office/Division	Office of the Chief Counsel
Phone Number	202-874-2306
Email Address	Sidney.Rocke@bep.gov

3. Who is the system manager for this system or application?	
Name / Title	Aaron Robison, Attorney Advisor
Office/Division	Office of the Chief Counsel
Phone Number	(202) 874-2058
Email Address	Aaron.Robison@bep.gov

4. Who is the Information System Security Manager who reviewed this document?	
Name / Title	Michael Pease, Chief
Office/Division	Office of Critical Infrastructure & Information Technology Security
Phone Number	(202) 874-2651
Email Address	Michael.Pease@bep.gov

5. Who is the Office/Bureau Privacy Officer who reviewed this document?	
Name / Title	Leslie Rivera-Pagán, Attorney Advisor (General)
Office/Division	Office of the Chief Counsel
Phone Number	202-874-2946
Email Address	Leslie.Rivera-Pagan@bep.gov

6. Who is the IT Reviewing Official?	
Name / Title	Jose Pena, Acting Manager
Office/Division	Office of Critical Infrastructure & Information Technology Security /Information Technology Audit & Compliance Division
Phone Number	(202) 874-3229
Email Address	Jose.Pena@bep.gov

Privacy Impact Assessment (PIA)

B. System Application/General Information

1. Does this system contain any PII? [] No [X] Yes

2. What is the purpose of the system/application?

The purpose of the Office of the Chief Counsel's System-Matters Tracking System (CCS-MTS) formerly known as Chief Counsel's System - Legal Cases is to assess the workload of the legal staff, track the status of matters assigned to the legal staff, and capture summary information (such as name of principal parties or subjects, case file numbers, and assignments) in matters such as litigation and/or administrative proceedings in which the Bureau of Engraving and Printing (BEP) is a party, and matters in which the Office of the Chief Counsel (OCC) must provide advice. In addition, these records are maintained to assist in providing legal advice to BEP Management regarding issues of compliance, investigation, and implementation of matters related to the BEP and the statutes and regulations administered by the BEP. The system also automatically issues an office file number to each matter, which the legal staff will use to track matters for recordkeeping purposes. CCS-MTS will afford the Office of the Chief Counsel the ability to inject workflows into each legal matter when necessary.

3. What legal authority authorizes the purchase or development of this system/application?

5 U.S.C. §§ 301, 5520a, 7301, 7351, 7353, 5 U.S.C. App. (Ethics in Government Act of 1978); 28 U.S.C. § 2672; 31 U.S.C. §§ 301, 321, 1353, 3721; 42 U.S.C. § 659; 44 U.S.C. § 3101 authorize the development of the CCS-MTS application.

4. Under which SORN does the system operate? (Provide name and number)

Some records in the system are covered by the following SORNs:

- a. Treasury .004 – Freedom of Information Act/Privacy Act Request Records;
- b. OGE/GOVT-1 - Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records;
- c. OGE/GOVT-2 - Executive Branch Confidential Financial Disclosure Reports;
- d. Treasury/BEP.002 – Personal Property Claim File;
- e. Treasury/BEP.006 – Debt Files of Employees; and
- f. Treasury/BEP.035 – Tort Claims against the United States of America.

The Office of the Chief Counsel will publish a new SORN in the Federal Register that will allow the agency to retrieve records using different personal identifiable information when using the IT and/or paper record system. In addition, the new SORN will contain new routines uses for situations in which BEP may share records on individuals covered by the SORN under the Privacy Act, 5 U.S.C. § 552a (a)(b)(3). The new SORN will be known as Bureau of Engraving and Printing Chief Counsel Files-Treasury/BEP.

Privacy Impact Assessment (PIA)

C. Data in the System

- 1. What categories of individuals are covered in the system? (e.g., employees, contractors, taxpayers, other)**

BEP employees, BEP contractors, members of the public, and/or individuals who are the subjects of, or are connected to, matters received or assigned to the OCC may be covered in the system.

- 2. What are the sources of information in the system?**

- a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other sources?**

The information is collected from already existing OCC subject matter and/or case files; BEP and OCC employees; Department of the Treasury employees; Federal, State, and/or Local agencies; judicial and administrative proceedings; tribal and foreign governments; labor organizations; congressional offices; public records; and parties and witnesses to disputed matters of fact or law.

- b. What Federal agencies are providing data for use in the system?**

The data comes from already existing Office of the Chief Counsel subject matter and/or case files, which may include documents from any Federal agency and/or court in which the BEP may be a named party in a matter, such as the EEOC, MSPB, FLRA, EPA, etc.

- c. What state and/or local agencies, tribal governments, foreign governments, or international organizations are providing data for us in the system?**

The data comes from already existing Office of the Chief Counsel subject matter and/or case files, which may include documents from any State and/or local agency, foreign government, or international organization in which the BEP may be a named party in a matter.

- d. From what other third party sources will data be collected?**

The data comes from already existing Office of the Chief Counsel subject matter and/or case files, which may include documents from any third party in which the BEP may be a named party in a matter.

- e. What information will be collected from employees, government contractors and consultants, and the public?**

This system will contain the following records:

Privacy Impact Assessment (PIA)

- Names, titles, and contact information of the parties and individuals involved, including phone and fax numbers, home and business addresses, and email addresses;
- Case and/or matter names, and case and/or matter identification numbers;
- Issues, descriptions, summaries, and statuses of cases and/or matters and assignments received in the OCC;
- Copies of relevant case and/or matter documents.

3. Accuracy, Timeliness, and Reliability

- a. **How is data collected from sources other than from Treasury records going to be verified for accuracy?**

Data collected from sources other than from Treasury records will be verified for accuracy with the source of the information.

- b. **Is completeness required?** No Yes

- c. **What steps or procedures are taken to ensure the data is current and not out-of-date?**

The Chief Counsel Staff continuously monitors the status of the matter on which they are working. If data appears to be out-of-date, the staff member will update the data, or reach out to the source of the data to ensure its accuracy.

- d. **Are the data elements described in detail and documented?** No Yes

The data elements are documented in the CCS-MTS Requirements Specifications document.

D. Attributes of the Data

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

All data collected is relevant and necessary for monitoring staff workload, and matter and/or case progression. In addition, the data is maintained to assist in providing legal advice to BEP Management.

2. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?** No Yes

Privacy Impact Assessment (PIA)

This system is only used as a tracking tool to monitor the assignment of work to legal staff and the status of that work. It only creates a recordkeeping file number and reports which are not descriptive enough to aggregate data. The file number assigned to the matter and/or case file will be used as a recordkeeping tool.

3. Will the new data be placed in the individual's record? No Yes
4. Can the system make determinations about employees/members of the public that would not be possible without the new data?

No.

5. How will the new data be verified for relevance and accuracy?

No new data is created.

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The system is protected from unauthorized access and use through group permissions, which determines the rights/privileges granted. The BEP IT security and OCC personnel maintain and audit this access control list. The Security Assessment and Authorization (SA&A) team is responsible for authoring a System Security Plan for all systems at BEP. Therefore, these security controls are documented in the CCS-MTS System Security Plan.

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

No processes are being consolidated.

8. How will the data be retrieved? Is the data retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data in the CCS-MTS application may be retrieved by name of the party or individual who are subjects to, or are connected to, matters received by or assigned to the OCC; name of the office; office file number; case number; case name; OCC staff name; case and/or matter status; case and/or matter subject; date the case and/or matter was opened; date the case and/or matter was closed; date the case and/or matter was modified; or by keyword search.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Privacy Impact Assessment (PIA)

Reports will be used to monitor the OCC legal staff workload and status of the subject matter and/or case files. The computerized records are maintained in the Chief Counsel's System. A printout of the data may be made. Access is limited to employees who have need for such records in the course of their work. All facilities where records are stored have access limited to authorized personnel.

E. Maintenance and Administrative Controls

- 1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The CCS-MTS is located in the DCF. Users access this information via the BEP Serena Business Manager application. Users in the WCF access the application through the network the same way as DCF users.

- 2. What are the retention periods of data in the system?**

Data and records are retained in accordance with NARA's General Records Schedule 23, Item 1 (N1-GRS-98-2 item 43).

- 3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Printed reports are retained for two years and then destroyed.

Paper records for disposal are destroyed by shredding or burning. Records in electronic form are electronically erased using accepted techniques.

The procedures used to facilitate this process are documented in BEP Circular No. 80-05, Records Management Program (2006); BEP Circular No. 80-05.3, Records Storage (2007); BEP Circular No. 80-05.4, Policies and Procedures for Electronic Records and E-Mail (2006).

- 4. Is the system using technology in ways the office or bureau has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, explain.**

No.

- 5. How does the use of this technology affect public/employee privacy?**

N/A.

- 6. Will the system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

Privacy Impact Assessment (PIA)

The system has the capability of tracking OCC legal staff assignments, and contains an audit trail capability that tracks when data is changed and by whom. The system also may identify an already existing subject matter and/or case file name or an administrative and/or court case name, which may include an individual's name. The system cannot locate or monitor individuals.

7. What kind of information is collected as a function of the monitoring of individuals?

Not applicable; the system does not provide the capability to monitor individuals.

8. What controls will be used to prevent unauthorized monitoring?

Not applicable; the system does not provide the capability to monitor individuals.

9. Under which SORN does the system operate? (Provide name and number)

Some records in the system are covered by the following SORNs:

- a. Treasury .004 – Freedom of Information Act/Privacy Act Request Records;
- b. OGE/GOVT-1 - Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records;
- c. OGE/GOVT-2 - Executive Branch Confidential Financial Disclosure Reports;
- d. Treasury/BEP.002 – Personal Property Claim File;
- e. Treasury/BEP.006 – Debt Files of Employees; and
- f. Treasury/BEP.035 – Tort Claims against the United States of America.

The Office of the Chief Counsel will publish a new SORN in the Federal Register that will allow the agency to retrieve records using different personal identifiable information when using the IT and/or paper record system. In addition, the new SORN will contain new routines uses for situations in which BEP may share records on individuals covered by the SORN under the Privacy Act, 5 U.S.C. § 552a (a)(b)(3). The new SORN will be known as Bureau of Engraving and Printing Chief Counsel Files-Treasury/BEP.

10. If the system is being modified, will the SORN require amendment or revision? Explain.

Some records will be covered by a new SORN and the others will be used in accordance with all existing SORNs (please see E.9.)

F. Access to Data

1. Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others).

OCC staff will be the primary users for the system. The system administrator will be a federal employee in the OCC. This person will be responsible for requesting access for

Privacy Impact Assessment (PIA)

users as appropriate via the BEN-IDM process. BEP OITO personnel maintain CCS-MTS. This team encompasses both federal as well as contractor personnel.

- 2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Users must complete BEP System Access Request Identity Manager Form requesting access to the system and be approved for access by authorized BEP personnel. Users are granted access based on their roles and need-to-know. Criteria, procedures, controls, and responsibilities regarding access to the system are documented in the access control portion of the CCS-MTS system security plan.

- 3. Will users have access to all data on the system or will the user's access be restricted? Explain.**

BEP's legal staff has access to CCS-MTS only. The administrators have access to privileged functions. Access restriction is based on role and responsibility.

- 4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? List procedures and training materials.**

Users participate in the mandatory Annual Privacy Awareness Training sponsored by the Department of the Treasury, Office of Privacy and Civil Liberties (OPCL) and the Records Management-Employees and Contractors Training sponsored by the Department of the Treasury, Office of Privacy, Transparency, and Records (OPTR).

- 5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?**

Contractors design, develop, and maintain the CCS-MTS Application for the BEP's Office of the Chief Counsel.

- 6. Do other systems share data or have access to the data in the system? If yes, explain.**

No. The CCS-MTS does not access or share any information with any IT systems within or outside of the BEP. The BEP legal staff will share the data in this system to the extent allowable under the new and above-referenced SORNs.

- 7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Chief Counsel, Office of the Chief Counsel.

- 8. Will other agencies share data or have access to the data in this system?**

Federal

State

Local

Other

Privacy Impact Assessment (PIA)

Yes. BEP legal staff will share the data in this system to the extent allowable under the new and above-referenced SORNs.

9. How will the data be used by the other agency?

The extent to which data in the system may be used by other agencies is as specified in the new and above-referenced SORNs.

10. Who is responsible for assuring proper use of the data?

Chief Counsel, Office of the Chief Counsel.

Privacy Impact Assessment (PIA)

The Following Officials Have Approved This Document

1. Program Manager/System Owner

Name: Sidney Rocke

(Signature)



Date

12/17/15

2. System Manager

Name: Aaron Robison

(Signature)



Date

12/17/15

3. Information System Security Manager

Name: Michael Pease

(Signature)

Date

4. Privacy Officer

Name: Leslie Rivera-Pagán

(Signature)



Date

12-17-15

5. IT Review Official

Name: Jose Pena

(Signature)

Date

6. Deputy Assistant Secretary for Privacy and Treasury Records (when necessary)

Name:

(Signature)

Date

Information for the Public regarding the Laboratory

1. The Laboratory is a public body.

2. The Laboratory is a public body.

3. The Laboratory is a public body.

4. The Laboratory is a public body.

5. The Laboratory is a public body.

15/11/12

[Handwritten signature]

6. The Laboratory is a public body.

7. The Laboratory is a public body.

8. The Laboratory is a public body.

9. The Laboratory is a public body.

[Handwritten signature]

10. The Laboratory is a public body.

11. The Laboratory is a public body.

12. The Laboratory is a public body.

13. The Laboratory is a public body.

14. The Laboratory is a public body.

15. The Laboratory is a public body.