Case Information Management System (CIMS)

Privacy Impact Assessment
for the
Case Information Management System

Issued by:
Kenneth Hendricks, Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: December 28, 2023

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Civil Division's Case Information Management System (CIV-CIMS), is a web-based system, designed to track the status and progress of the work of the legal staff regarding the various stages of all of the Civil Divisions' cases, from the initial receipt of a case, matter, and claim, through the pre-file and trial court stages, and, if necessary, through appellate courts. CIMS contains various types of case tracking information that include personally identifiable information (PII), which is the reason why this Privacy Impact Assessment was conducted. The system does not contain underlying records from the case files, which are maintained in other Civil Division systems. For specific programs, such as Radiation Exposure Compensation Act (RECA) and Immigration, the system stores additional PII that helps the Civil Division's components track related claims and cases.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The Civil Division serves as the lead civil litigation component of the Department of Justice. This includes the representation of government agencies as well as representation of the federal government in a wide range of civil and administrative actions. As such, the litigation managed by the Division covers a wide range of types of matters, claims and cases, usually creating a need to store personally identifiable information.

As noted above, CIV-CIMS is designed to track the status and progress of the work of the legal staff from the initial receipt of a case, matter, and claim, through the pre-file and trial court stages, and, if necessary, through appellate courts. This data serves as the basis for such system functions as generating reports describing characteristics of the caseload, distribution among litigation areas, dollars at issue, subject matter, referring agency, and case assignment roles and handling; responding to ad hoc questions on specific cases or groups of cases; automatically generating draft letters that can be sent to U.S. Attorneys and referring-agencies related to specific cases; and conducting database searches in order to route case correspondence to the appropriate Civil Division attorney.

The system includes Social Security Numbers and other PII needed to track claims and cases related to the RECA program. Immigration related cases may be tracked using the associated alien registration number.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	5 U.S.C. § 301 (agency operations); 28 U.S.C. §§ 514-19; 42 U.S.C. § 2210 note (Radiation Exposure Compensation Act).
Executive Order	
Federal regulation	28 C.F.R. §§ 0.45-0.49

Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

<u>Section 3</u>: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). <u>Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.</u>

(1) General Categories of Information that May Be Personally Identifiable	**(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)**	**(3) The information relates to:**
		A. DOJ/Component Employees, Contractors, and Detailees;
		B. Other Federal Government Personnel;
		C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);
		D. Members of the Public - Non-USPERs
			(4) Comments

Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C & D	Full names of DOJ personnel and individuals mentioned in case information.
Date of birth or age	X	C & D	Dates of birth of individuals mentioned in case information.
Place of birth			
Gender			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C & D	Social Security Numbers of individuals mentioned in case information.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C & D	Alien registration numbers of individuals mentioned in case information.
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C & D	Mailing addresses of individuals mentioned in case information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to:
		A. DOJ/Component Employees, Contractors, and Detailees;
		B. Other Federal Government Personnel;
		C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);
		D. Members of the Public - Non-USPERs
			(4) Comments

Personal e-mail address			
Personal phone number	X	C & D	Personal phone numbers of individuals mentioned in case information.
Medical records number			
Medical notes or other medical or health information	X	C & D	Medical records number of individuals mentioned in case information.
Financial account information	X	C & D	CIMS may contain financial information about an individual as it pertains to an award/outcome of a case.
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C & D	Case Name, Allegation and Docket Number for some cases are tracked in CIMS
Whistleblower, e.g., tip, complaint, or referral	X	C & D	Whistleblower Name is tracked for False Claims Act (FCA) cases.
Grand jury information	X	C & D	Grandy Jury Party is tracked for some cases.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to:
		A. DOJ/Component Employees, Contractors, and Detailees;
		B. Other Federal Government Personnel;
		C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);
		D. Members of the Public - Non-USPERs
			(4) Comments

Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			System log information of system users.
- **User ID**	X	A	
- **User passwords/codes**			
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	
Phone		Email			
Other (specify): Information is not collected directly from the individual into the system. Information is collected from within the government component.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	Civil Division employees and contractors with assigned roles and permissions can only access information in the system by logging into CIV-CIMS.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

The CIMS aggregate and summary reports published on data.gov do not contain any PII.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Generalized notice is provided via the System of Records Notice (SORN). Depending on the type of case involved, the following SORNs may apply:

- CIV-001, Civil Division Case File System, last published in full at: 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), available at: https://www.gpo.gov/fdsys/pkg/FR-1998-02-20/pdf/98-4206.pdf.
- CIV-002, Civil Division Case File System: Customs Litigation, last published in full at: 45 Fed. Reg. 2215, 217 (Jan. 10, 1980), available at: https://www.justice.gov/opcl/docs/45fr2217.pdf.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals cannot voluntarily participate in the use of their information in Civil Division cases. CIMS does not collect information directly from individuals.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals and their representatives can request access to information under the Freedom of

Information Act or the Privacy Act by submitting requests directly to the Civil Division (see https://www.justice.gov/civil/webform/civil-division-foia-e-request-form for submission information). An individual can submit a Privacy Act Amendment or Correction request of their first-party information (see https://www.justice.gov/opcl/doj-privacy-act-requests for submission information). Note, however, that much of the information in CIMS may be subject to Exemption 5 of the FOIA 5 U.S.C. 552(b)(5) (protecting work-product and other litigation privileges) as well as to Section 552a(d)(5) of the Privacy Act 5 U.S.C. 552a(d)(5) (excluding from access rights under the Privacy Act information compiled in reasonable anticipation of a civil action or proceeding).

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** ATO date: March 12, 2021 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** CIMS is categorized as a moderate system based on its review of the aggregate impact for the confidentiality, integrity, and availability.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The highest sensitivity information contained in this system pursuant to the Federal Information Processing Standards (FIPS) security categorization(s), as defined in NIST Special Publication 800-60, Guide for Mapping Types of Information, and Information

	Systems to Security Categories, is Moderate and matches the most sensitive information in the system, per the 'high water mark' standard. CIMS operates within the boundary of the Civil Division and is subject to full system monitoring and auditing in accordance with the Department of Justice guidelines. System documentation supporting these activities are maintained within the department's system of records, Cyber Security Assessment & Management (CSAM) tool.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** System logs are captured in Splunk, reviewed monthly and stored in SharePoint.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. All contractors granted access to CIV-CIMS are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role.
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: There is no additional Privacy-related training specific to CIV-CIMS.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Administrative Controls: Authorized users are assigned a role that gives them data access on a need-to-know basis to accomplish their duties. A user's access to CIV-CIMS is ended within twenty-four hours of termination from the JCON Network. Additionally, each CIV-CIMS user is part of Justice Consolidated Office Network (JCON). JCON requires each user to attend Civil Division's Computer Security Awareness Training (CSAT) to continue to bring more awareness to each user's responsibility in protecting personally identifiable information. At the end of the annual training, the users are required to sign the Rules of Behavior (ROB) form that outlines each user's responsibility in safeguarding PII.

Technical Controls: Each PII requirement is vetted by management and determined to be necessary before authorizing its addition to CIV-CIMS. Once an element of PII is determined to be part of a requirement, system administrators ensure that Create, Read, Update, and Delete (CRUD) matrix is created to determine the CIMS roles that would perform each CRUD function. Information access is thoroughly checked by manual and automated testing to ensure that system and roles-based security is enforced according to requirements in the CRUD matrix.

Physical Security: The buildings that host CIV-CIMS servers are manned by security guards 24/7, who allow building access to authorized personnel only. The server rooms in the buildings are secured by PIV card reader security and only authorized users with a valid PIV card can access them. Access to all server rooms is logged and monitored by JCON. All the data collected are stored in Civil Division's data center under the control of the Chief Information Officer's (CIO) office, and has neither public interface nor access beyond Civil Division employees and contractors.

Database access is limited to a handful of Civil Division employees and contractors who have administrative access to the database servers. These employees and contractors require a special administrative PIV card to access the database directly. Each administrative user undergoes separate annual Rules of Behavior (ROB) training, and is required to sign a rules and responsibility acknowledgement in safeguarding the CIV-CIMS data stores.

Any transmittal of CIMS data within the Division is protected by the above-noted security measures. CIV-CIMS does not connect to nor transmit information to external systems.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

The Civil Division maintains the CIMS data pursuant to the following records retention schedule: Civil Division Case Management System, Number N1-060-05-13, available at https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0060/n1-060-05-013_sf115.pdf.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. _X_ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

The following SORNs apply:

- CIV-001, Civil Division Case File System, last published in full at: 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), available at: https://www.gpo.gov/fdsys/pkg/FR-1998-02-20/pdf/98-4206.pdf.
- CIV-002, Civil Division Case File System: Customs Litigation, last published in full at: 45 Fed. Reg. 2215, 217 (Jan. 10, 1980), available at: https://www.justice.gov/opcl/docs/45fr2217.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

A. Potential Risks Related to Unauthorized Information Collection

There is a privacy risk arising from the over-collection of information. In order to mitigate this, CIV-CIMS only stores data determined to be necessary to meet its primary mission of tracking the status and progress of the work of the legal staff from the initial receipt of a case, matter or claim, through the pre-file and trial court stages, and, if necessary, through appellate courts.

Each PII element is vetted by management and determined to be necessary before authorizing its addition to CIV-CIMS. Once an element of PII is determined to be part of a requirement, system administrators ensure that Create, Read, Update and Delete (CRUD) matrix is created to determine the CIMS roles that would perform each CRUD function. Information access is thoroughly checked by manual and automated testing to ensure that system and roles-based security is enforced according to requirements in the CRUD matrix.

Collection of victim's and claimant's Social Security Number and other identifiable information for RECA is required to minimize false claims by checking DoNotPay.gov system, and to make RECA payments to claimants.

B. Potential Risks Related to the Unauthorized Use of Information

Privacy risks regarding unauthorized access to personally identifiable information in CIMS is minimized by controlling the access to the information through roles-based security rules. In addition, each CIV-CIMS user is part of Justice Consolidated Office Network (JCON). JCON requires each user to attend Civil Division's Computer Security Awareness Training (CSAT), to continue to bring more awareness to each user's responsibility in protecting personally identifiable information. The CIV-CIMS security administration controls terminate access to CIV-CIMS for the users who are not part of JCON, within twenty-four hours.

C. Potential Risks Related to the Unauthorized Dissemination of Information

There is a privacy risk of inadvertent exposure of PII when information is disseminated. In order to mitigate this risk, any transmittal of CIMS data within the Division is protected by the above-noted security measures. Additionally, CIV-CIMS does not connect to nor transmit information to external systems.