[CIV-Civil Data Analytics System (CIV-CDAS)]

Privacy Impact Assessment
for the
CIV-Civil Data Analytics System (CIV-CDAS)

Issued by:
Kenneth Hendricks, Senior Component Official for Privacy

Approved by: Hannah Mayer
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: January 7, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Civil Division uses the Civil Data Analytics System (CDAS) as a platform for investigating malfeasance, enforcing laws, and elevating performance across program and divisional domains. The Civil Division also uses CDAS to facilitate collaboration between case teams and Expert Witnesses and swiftly deploy tailored software solutions to address unique requirements beyond the Division's existing application suite. This capability enhances the user experience and maintains data within the Division's technology boundary, thereby accommodating ever-evolving technology needs while adhering rigorously to federal and departmental information system security protocols. CDAS is also instrumental in optimizing performance at programmatic and divisional echelons by analyzing data collected from internal programs, creating actionable insights aimed at driving operational excellence.

Pursuant to the privacy provisions of the E-Government Act of 2002, the Civil Division has prepared a Privacy Impact Assessment (PIA) for this system because it collects, maintains, and disseminates information in identifiable form. CDAS serves as a repository for financial and healthcare data, encompassing Personally Identifiable Information (PII) and Personal Health Information (PHI) sourced from legal process as well as open and proprietary sources. This includes litigation-related data, vendor contributions, and data produced from collaborating agencies. Analysts use this data to investigate complex consumer fraud, deceptive trade practices and telemarketing violations, Veterans and US servicemember fraud, and other violations, while Civil Division attorneys decide what information should be added to CDAS as a function of those use cases and investigations.

Additionally, CDAS stores data collected from internal programs to assist leadership in streamlining operations and elevating performance. CDAS ingests and securely stores these diverse datasets within the Civil Division's Amazon Web Services environment on GovCloud, which is specifically designed to meet stringent federal information security requirements. This environment ensures the protection and integrity of sensitive data in a way that is tailored to the security needs of federal agencies.

Within this compliant infrastructure, CDAS facilitates the creation of court-admissible analytical insights. Employing a multifaceted approach, CDAS seamlessly integrates traditional and state-of-the-art methodologies. From foundational data exploration and descriptive statistics to the more sophisticated development of machine learning models, CDAS is useful for identifying and predicting patterns. Through this comprehensive framework, CDAS not only safeguards sensitive information but also empowers the Civil Division with actionable data tailored to legal and regulatory contexts.

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. As such, the types of litigation managed by the Division cover a wide range of types of matters and cases, creating expansive and diverse data sets in the process of this representation. This includes different file types collected or received from collaborating agencies to social media data and cellular device data. The Civil Division also receives significant volumes of data from third parties in a wide range of formats for review and analysis. These data are part of the civil law enforcement litigation lifecycle, including investigation and discovery.

The Civil Division is also responsible for administering high-profile federal programs Congressional funding for these programs is on the scale of billions of dollars and operationalizing them entails managing complex systems with interdependent workflows. Using data to ensure that these programs operate optimally is key to the Civil Division's mission, mitigates fraud risk, and ensures that program resources are managed efficiently.

CDAS supports this dynamic mission as a robust digital platform for cultivating and automating data-centric insights. CDAS leverages cloud-based infrastructure to offer the Division inherent advantages in speed and scalability. This facilitates in turn the creation of innovative tools and methods tailored to meet complex federal, divisional, and legal-judicial requirements. CDAS' capabilities encompass the generation of data-powered insights using state-of-the-art tools and techniques, offer a software-as-a-service model to quickly satisfy constantly evolving technology needs on-demands, and support comprehensive data analyses spanning diverse divisional domains to continuously assess and enhance mission outcomes.

CDAS' capabilities include collecting, processing, hosting, visualizing, and producing structured and unstructured data. By harnessing these capabilities, the Civil Division can navigate intricate investigation and litigation processes with confidence and agility, collaborate seamlessly with external partners, and streamline and continuously improve its operations.

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; 28.
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)	

Section 3: 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). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of 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
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	Information contained in litigation data including agency investigative files and discovery. In instances where CIV personnel are counsel to other DOJ components or in limited instances otherwise, litigation data may include certain CIV personnel information.
Date of birth or age	X	A, B, C, D	Information contained in litigation data including agency investigative files and discovery. Litigation data may include certain CIV personnel information.
Place of birth	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Gender	X	A, B, C, D	Information contained in litigation data including agency investigative files and discovery. Litigation data may include certain CIV personnel information.
Race, ethnicity, or citizenship	X	A, B, C, D	Information contained in litigation data including agency investigative files and discovery. Litigation data may include certain CIV personnel information.
Religion	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Social Security Number (full, last 4 digits or otherwise truncated)	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Tax Identification Number (TIN)	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.

(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
Driver's license	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Alien registration number	X	C, D	Information contained in litigation data including agency investigative files and discovery.
Passport number	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Mother's maiden name	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Vehicle identifiers	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Personal mailing address	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Personal e-mail address	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Personal phone number	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Medical records number	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Medical notes or other medical or health information	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Financial account information	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Applicant information	X	A, B, C, D	Information contained in litigation data including agency investigative files and discovery. Litigation data may include certain CIV personnel information.
Education records	X	A, B, C, D	Information contained in litigation data including agency investigative files and discovery. Litigation data may include certain CIV personnel information.
Military status or other information	X	A, B, C, D	Information contained in litigation data including agency investigative files and discovery. Litigation data may include certain CIV personnel 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
Employment status, history, or similar information	X	A, B, C, D	Information contained in litigation data including agency investigative files and discovery. Litigation data may include certain CIV personnel information.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Certificates	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Legal documents	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Device identifiers, e.g., mobile devices	X	A, B, C, D	Information contained in litigation data including agency investigative files and discovery. Litigation data may include certain CIV personnel information.
Web uniform resource locator(s)	X	C, D	Information contained in litigation data including agency investigative files and discovery.
Foreign activities	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Juvenile criminal records information	X	C, D	Information contained in litigation data including agency investigative files and discovery.
Civil law enforcement information, e.g., allegations of civil law violations	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Whistleblower, e.g., tip, complaint, or referral	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Grand jury information	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Procurement/contracting records	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Proprietary or business information	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.

(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
Location information, including continuous or intermittent location tracking capabilities	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
Biometric data:			
- **Photographs or photographic identifiers**	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
- **Video containing biometric data**	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
- **Fingerprints**	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
- **Palm prints**	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
- **Iris image**	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
- **Dental profile**	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
- **Voice recording/signatures**	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
- **Scars, marks, tattoos**	X	B, C, D	Information contained in litigation data including agency investigative files and discovery.
- **Vascular scan, e.g., palm or finger vein biometric data**	X	B C, D	Information contained in litigation data including agency investigative files and discovery.
- **DNA profiles**	X	C, D	Information contained in litigation data including agency investigative files and discovery.
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A, B, C	
- **User passwords/codes**			CDAS does NOT store user passwords/code. CDAS will require password reset.
- **IP address**	X	A, B	
- **Date/time of access**	X	A, B	For administrative logs and user account management.
- **Queries run**	X	A, B	Search and coding history.
- **Contents of files**	X	A, B, C, D	Information contained in litigation data including agency investigative files and discovery.

(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
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Because of the varied nature of the records relevant to litigation activities, other types of PII not listed above may be collected, maintained, or disseminated.

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):					

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	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): Through the litigation process, including in response to authorized legal process (e.g., subpoena, Request for Production, etc.)					

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	X	X	Data will be shared through role-based access as required for litigation purposes in specific cases and program administration and governance.
DOJ Components	X	X	X	Data will be shared through role-based access as required for litigation purposes in specific cases and program administration and governance.
Federal entities	X		X	Data will be shared through role-based access as required for litigation purposes in specific cases and program administration and governance.
State, local, tribal gov't entities	X			Data will be shared through role-based access as required for litigation purposes in specific cases. Persons who get direct log-in access and experts with whom CIV shares information will be required to sign the DOJ Rules of Behavior, confidentiality agreement, and to review the transcript of OPCL's privacy training module and the Cybersecurity Awareness Training as part of their access to a CIV information system or CIV information.
Public				

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.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Work products (e.g., reports, data visualizations, etc.) may be shared as part of the litigation process. Persons who get direct log-in access and experts with whom CIV shares information will be required to sign the DOJ Rules of Behavior, confidentiality agreement, and to review the transcript of OPCL's privacy training module and the Cybersecurity Awareness Training as part of their access to a CIV information system or CIV information.
Private sector				
Foreign governments				
Foreign entities				
Other (specify): Expert Witness	X			Data will be shared through role-based access as required for litigation purposes in specific cases. Persons who get direct log-in access and experts with whom CIV shares information will be required to sign the DOJ Rules of Behavior, confidentiality agreement, and to review the transcript of OPCL's privacy training module and the Cybersecurity Awareness Training as part of their access to a CIV information system or CIV information.

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.

No, CIV will not be releasing the data to the public for "Open Data" purposes at this time.

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:

- DOJ-002, Department Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999) and amended at 82 Fed. Reg. 24147 (May 25, 2017).
- CIV-001, Civil Division Case File System, 63 Fed. Reg. 8659-8665 (Feb. 20, 1998), as amended at 82 Fed. Reg. 24147 (May 25, 2017).

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 how their information gets used in CDAS because CDAS is not a primary source for collecting, using, or disseminating information. Data in CDAS exists as a copy of itself from other systems, sources, and programs (e.g., CIV-JCON).

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/foia 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).

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: Underway, currently pursuing ATT as an interim milestone. **If an ATO has not been completed, but is underway, provide status or expected completion date:** ATO is underway and expected to be completed by 9/30/2025. **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:**
X	**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:** CDAS is subject to ATO process, which is expected to complete by 9/30/2025.
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:** CDAS is categorized as a high system based 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 **HIGH** and matches the most sensitive information in the system, per the 'high water mark' standard. CDAS operates within the boundary of Civil Division's cloud service provider, Amazon Web Services as a Platform-as-a-Service, where it 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 record, Justice Continuous Active Monitoring (JCAM), formerly known as 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:** CDAS uses a combination of services like CloudWatch and CloudTrail to continuously monitor activity logs in compliance with federal information security standards.
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 CDAS are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role.
X	**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:** Additional training on this system is available to both internal personnel and expert witnesses. The training explains the roles-based access system and appropriate permissions to promote information security.

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?

All Civil Division personnel and external system users sign the DOJ Rules of Behavior prior to being granted access to the platform and annually thereafter as required during the lifecycle of the case. Information in CDAS is encrypted both in storage and transit.

CDAS uses distinct role-based profiles to provide only the permissions needed to achieve each user's required level of activities. Such roles include an Account Administrator who controls the provision of individual user accounts, and varying levels of privileges assigned to individual users to access tools and datasets on a controlled basis. CDAS also uses Amazon Web Services' Identity and Access Management controls, network access controls, and security group policies to limit access to virtually every aspect of the platform as needed.

This means that users may access only the platform aspects to which they have been granted privileges. Non-authorized users may not access unauthorized aspects of the platform. Aspects of the platform include but are not limited to viewing and editing data objects and using tools. Meanwhile, inactive users are automatically deactivated after 90 days as a system control, and all user accounts are reviewed quarterly to proactively enforce user account management.

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 data in CDAS consists of copies of information from the underlying litigation and program files, and analytical output that is derived from such copied information. CDAS stores data as long as needed, from pre-case investigation to case opening and case closure, and on a rolling basis to enhance internal program performance. The source file information from which the CDAS copies are made, and derivative analytical CDAS output, will be retained in accordance with the records schedules associated with the source materials (e.g., litigation files, program data, etc.), including any derivative work products which will be marked as part of the records management review and retention practices. Such files if required for retention will become part of the electronic files stored and subsequently disposed according to NARA guidelines.

Record retention policies depend on the federal record status and the classification of the type of case file. Retention periods for case files range from approximately five years to permanent. Temporary records are destroyed at the end of the retention period, and permanent records are transferred to the custody of the National Archives and Records Administration at intervals note din the records retention schedules. Non-records, such as duplicates and unnecessary discovery or other submitted documents, are destroyed when no longer needed for convenience of reference. The Department of Justice record retention schedules are published at: https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060.

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:

- DOJ-002, *Department Computer Systems Activity and Access Records*, last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999) and amended at 82 Fed. Reg. 24147 (May 25, 2017).
- CIV-001, *Civil Division Case File System*, 63 Fed. Reg. 8659-8665 (Feb. 20, 1998), as amended at 82 Fed. Reg. 24147 (May 25, 2017).

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?

I. *Risks Related to Information Collection*:

There are privacy risks associated with the over-collection of information. In order to mitigate these risks, CDAS follows data minimization practices aimed at retaining only necessary data, and either purging or archiving unused data as a function of the corresponding case life cycle. If a case closes, the relevant case data is expunged from CDAS and passed to the applicable data steward for retention with the source material if required under the applicable records schedule; if an internal program reaches end-of-life, its performance data in CDAS is removed and retained according to the applicable program records retention schedule. CDAS also uses data masking techniques to hide PII where and when it is not necessary.

II. *Risks Related to Use of Information*:

Potential privacy risks arising from the Department's use of the information in CDAS include unauthorized access to the information, improper disposal of the information, and unauthorized disclosure of the information. To mitigate these risks, CDAS implements strict identity and access management controls using a combination of role-based permissions, security groups, and activity log monitoring. End users are associated with predefined roles that correspond to security policies, which in turn limit the extent to which any one user may interact with CDAS in its entirety.

Users may access only the platform aspects to which they have been granted privileges. Non-authorized users may not access unauthorized aspects of the platform. Aspects of the platform include but are not limited to viewing and editing data objects and using tools. Meanwhile, inactive users are automatically deactivated after 90 days as a system control, and all user accounts are reviewed quarterly to proactively enforce user account management.

III. *Risks Related to Dissemination of Information*:

There is a potential risk to privacy that could result from unauthorized disclosure of the information within CDAS. Information in CDAS is inherently linked to privacy risks. These include unauthorized access to sensitive data, potential data breaches, and the misuse of data in CDAS. In order to mitigate this risk, regular audits and log monitoring are conducted to detect and address security issues, and all users agree to the DOJ Rules of Behavior and must maintain currency against all DOJ cybersecurity and privacy-related training requirements. Additional training on this system is available to both internal personnel and expert witnesses. The training explains the roles-based access system and appropriate permissions to promote information security. CDAS also uses a combination of services like CloudWatch and CloudTrail to continuously monitor activity logs in compliance with federal information security standards. Persons who get direct log-in access and experts with whom CIV shares info would be required to sign the DOJ Rules of Behavior, confidentiality agreement, and to review the transcript of OPCL's privacy training module and the Cybersecurity Awareness Training as part of their access to a CIV information system or CIV information.