Office of the Solicitor General

Privacy Impact Assessment
for the
Automated Docket System 2.0

Issued by:
Valerie H. Yancey, Executive Officer

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

Date approved: May 22, 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 Office of the Solicitor General (OSG) is tasked to supervise and conduct government litigation in the United States Supreme Court. Virtually all such litigation is channeled through OSG and is actively conducted by the Office. The United States is involved in approximately two-thirds of all the cases the U.S. Supreme Court decides on the merits each year. Automated Docket System 2.0 (ADS2) contains data on each case, petition, recommended information, and legal matter, including petitioner/respondent, case number, division/agency, case attorneys, various filing and court dates, disposition, proceeding lists, and case summary. The data input into ADS2 is used to track the process of each entry unto its completion. Pursuant to the privacy provisions of the E-Government Act of 2002 and the Office of Management and Budget's (OMB) implementing guidance (M-03-22), OSG has prepared this Privacy Impact Assessment because ADS2 collects, maintains, and disseminates information in identifiable form. Specifically, the documents contained within ADS2 include names and contact information of Department of Justice (DOJ) personnel and members of the public, such as attorneys, petitioners, and respondents.

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.

ADS2 is a browser interfaced application used by the Case Management Section (CMS), OSG to track and maintain information regarding Supreme Court cases, petitions not yet filed, recommendations and unnumbered matters. CMS serves the Solicitor General (SG) by supervising all aspects of Government litigation by which the SG executes their many executive functions. It serves the attorneys within OSG by advising them and insisting upon their adherence to Court procedural rules. ADS2 contains data on each case, petition, recommended information, and legal matter, including petitioner/respondent, case number, division/agency, case attorneys, various filing and court dates, disposition, proceeding lists, and case summary.

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	Congress has provided for the appointment of the Solicitor General in 28 U.S.C. § 505, and has specifically authorized the Solicitor General to handle cases in 28 U.S.C. §§ 517 and 518, which allow the Attorney General to delegate or assign other duties to the Solicitor General (and other attorneys and employees of OSG) in 28 U.S.C. §§ 510, 515-519, and has authorized the Solicitor General or a Deputy Solicitor General to approve certain criminal appeals in 18 U.S.C. § 3742(b).
Executive Order	
Federal regulation	Consistent with those statutes, DOJ regulations also give the Solicitor General certain authorities. See 28 C.F.R. §§ 0.20-0.21, 0.137, 0.163.
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	Names from past and current federal employees and officers. Names of members of the public is included like petitioners, respondents, and opposing counsels.
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C, D	Information about past and current federal employees and officers. Information about members of the public is also included like petitioners, respondents, and opposing counsels.
Personal e-mail address	X	A, B, C, D	Information about past and current federal employees and officers. Information about members of the public is also included like petitioners, respondents, and opposing counsels.
Personal phone number	X	A, B, C, D	Information about past and current federal employees and officers. Information about members of the public is also included like petitioners, respondents, and opposing counsels.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant 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
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			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			

(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
- **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:			
- **User ID**			
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**			
- **Queries run**			
- **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	X	Online	
Phone		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	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		X	Attorneys within OSG will personally retrieve documents
DOJ Components	X			Documents are shared by OSG attorneys on a case-by-case basis with DOJ attorneys in other components. The documents are usually shared by email or a JEFS portal depending on the volume. The sharing allows for collaboration on cases with other DOJ attorneys.
Federal entities	X			Documents are shared by OSG attorneys on a case-by-case basis with attorneys working for other Federal entities. The documents are usually shared by email or a JEFS portal depending on the volume. The sharing allows for collaboration on cases with other attorneys working for other Federal entities.
State, local, tribal gov't entities				

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.**
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
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.

Not Applicable.

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.

No particularized notice is provided.

Except for the recommendations from the SG or the Deputies, the information is already in the public domain as published by various courts and can be accessed by visiting the court in question or searching for the information through various online legal services.

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.

No opportunities are available for individuals to voluntarily participate in the collection or otherwise regarding their information considering it is already in the public domain as

published by various courts. The information can be accessed by visiting the court in question or searching for the information through various online legal services.

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.

No procedure exist which allows for any individuals to gain access to information in the system given that ADS2 is a closed system only available to those with the appropriate permissions. Moreover, the information considered is already in the public domain.

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):** August 1, 2022 **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:** ADS2 has a FIPS categorization of Low in accordance with the high-water mark standard.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:**

	The ADS 2.0 application is hosted on Justice Case Application (JCAP) servers and managed by the Application Technical Services (ATS) team. ATS manages the application and all patches, updates, etc. are done by the ATS team. The Vulnerability Management Team (VMT) assists with ensuring the application is scanned monthly. Audit logs are logged and monitored by ATS and the Information Systems Security Officer (ISSO).
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:** Audit logs are reviewed weekly by the assigned Information Systems Security Officer (ISSO) and the Justice Case Application Platform (JCAP) ISSO since the application sits on JCAP servers.
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**.
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:** There is no specific training provided by OSG as it relates to ADS2. Every user is instructed, individually, by their supervisor on the system's use and methods to safeguard any information contained therein. Moreover, every user is required to complete the Cybersecurity Awareness Training (CSAT) as required by OCIO, DOJ.

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?

ADS2 is a closed system available to only those who have been provided access by the CMS Supervisor, and there exist no outside connections of concern. The control of any PII in the system is in the hands of the users who are individually given authorization from the CMS Supervisor and have completed CSAT training. Additionally, audit logs are reviewed weekly to ensure compliance with privacy and security standards.

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.)

A case tracking record schedule that will cover the records maintained in ADS2.0 is in the National Archive and Records Administration (NARA) approval process.

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).

__X___ No. _____ Yes.

Searches are conducted using Supreme Court case numbers, subject categories, or other terms that are not personal identifiers.

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:

Not Applicable.

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?

There are minimal privacy risks associated with the use of ADS2, however, there is a privacy risk associated with unauthorized access to the consolidated public information within the system. In order to mitigate this risk, ADS2 provides access only to those with specific permissions as granted by the CMS Supervisor and have completed CSAT training. Once the relevant matter is closed, files related to the matter are retained in the system but removed from the active file thus rendering them moot. Additionally, audit logs are reviewed weekly to ensure compliance with privacy and security standards. Moreover, the PII contained in the system is information that is already in the public domain, so its potential release is not expected to cause additional privacy risk or undue burden.