Antitrust Division

Privacy Impact Assessment
for the
ATR iManage Document Management System-Cloud (ATR IDMS-C)

Issued by:
Sarah Oldfield
Senior Component Official for Privacy

Approved by: Katherine M. Harman-Stokes
Director (Acting), Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: February 29, 2024

(May 2022 DOJ PIA Template)

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

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 Antitrust Division (ATR) uses the iManage Document Management System-Cloud (IDMS-C) (Infrastructure as a Service) as a virtual librarian to file, manage, and securely access ATR documents. ATR currently has over 4 million documents in iManage that can be searched and cataloged. These documents comprise, but are not limited to, investigative files, litigation and court materials, internal personnel files, records, and other administrative data.

Once a document is entered into IDMS-C, it is indexed and searchable by content as well as metadata. Additionally, IDMS-C tracks data about the documents, such as creation, modification, and whether a document is "checked-out." Security measures are also applied when files are saved to ensure document integrity and availability. IDMS-C is a non-public system, with access limited to Division personnel.

This Privacy Impact Assessment (PIA) was prepared because IDMS-C contains information in identifiable form relating to DOJ personnel and members of the public. As required by Section 208 of the E-Government Act of 2002, this PIA explains how such data is stored, managed, and shared, in accordance with Federal privacy and information protection guidelines.

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.

ATR IDMS-C operates as a subsystem within ATR's Cloud Computing Environment's (ATR CCE) network boundary. ATR IDMS-C stores information in support of ATR's mission to enforce antitrust laws. It enables users to combine emails, office files, and case documents into project files for matter-centric collaboration to assist ATR in more effectively managing and controlling data and documents.

All authorized ATR personnel are provided initial accounts and ATR IDMS-C-specific

training upon onboarding. The primary users of ATR IDMS-C are ATR attorneys and paralegals, who use the database to store, manage, and manipulate documents collected and generated by ATR personnel in connection with investigations and cases. Other users include ATR office support personnel such as Human Resources (HR), Acquisitions Management Section, and Budget and Fiscal Section personnel, who use the application to manage and store day-to-day office management, accounting, and personnel files. Once users establish files and folders, they have the ability to grant or deny other users access to those controlled files.

Data in ATR IDMS-C, which may include investigative files, litigation and court materials, internal personnel files, records, and other administrative data, is kept in the form of general records, emails, memos, and other documents. Because ATR IDMS-C is not the primary information system in which ATR stores documents obtained in or relating to an investigation or litigation, certain documents are stored only as copies rather than original documents within the system.

ATR IDMS-C processes and stores a variety of personally identifiable information (PII). For example, documents from investigative and case files may contain PII about members of the public, such as personal contact information or date of birth. Documents in ATR IDMS-C may also contain medical or health information, or tax identification numbers, if relevant to a particular matter. Documents maintained by ATR human resources personnel, such as applicant and personnel records, contain the standard PII necessary for human resources administration, including dates of birth, social security numbers, personal contact information, employment history, salary and benefit information, and performance ratings.

ATR uses the FileSite version (Full client installation on the workstation), which is accessible to all ATR personnel. ATR IDMS-C is managed and supported by the Litigation Support Section (LSS) and the Engineering and Operations Section (EOS) within ATR's Executive Office.

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	28 C.F.R. §§ 0.40, General functions, and 0.41, Special functions
Executive Order	
Federal regulation	
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	
Date of birth or age	X	A, C, D	
Place of birth	X	A, C, D	
Gender	X	A, C, D	
Race, ethnicity, or citizenship	X	A, C, D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A	HR stores and accesses SSNs of ATR employees in ATR IDMS-C
Tax Identification Number (TIN)	X	C, D	
Driver's license	X	C, D	
Alien registration number	X	C, D	
Passport number	X	C, D	
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, C, D	
Personal e-mail address	X	A, C, D	
Personal phone number	X	A, C, D	
Medical records number	X	A, C, D	
Medical notes or other medical or health information	X	A, C, D	
Financial account information	X	A, C, D	
Applicant information	X	A, C, D	
Education records			
Military status or other information	X	A, C, D	
Employment status, history, or similar information	X	A, C, D	

(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 performance ratings or other performance information, e.g., performance improvement plan	X	A	
Certificates	X	C, D	
Legal documents	X	C, D	
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	C, D	
Foreign activities	X	C, D	
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C, D	
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C, D	
Whistleblower, e.g., tip, complaint, or referral	X	C, D	
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C, D	
Procurement/contracting records	X	C, D	
Proprietary or business information	X	C, D	
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**			

(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
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:[1]			
- **User ID**	X	A, C, D	
- **User passwords/codes**			
- **IP address**	X	A, C, D	
- **Date/time of access**	X	A, C, D	
- **Queries run**	X	A, C, D	
- **Contents of files**	X	A, C, D	
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):					

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

[1] System administrators include ATR account managers (Category A individuals) and vendor system administrators (Category C, D individuals). Vendor administrators have no access to ATR systems or passwords.

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	✓		✓	ATR personnel will share information stored in ATR IDMS-C among ATR personnel and offices on a case-by-case basis via email. ATR users have control over their documents within ATR IDMS-C and can grant access to others to view and manipulate documents they own (via direct log-in access). However, they are required to abide by organizational rules for sharing of case data and will need Section Chief/Assistant Chief approval to share case information outside the authorized group.
DOJ Components	✓			ATR users will share ATR IDMS-C information with other DOJ components on a case-by-case basis via email in accordance with organizational rules.
Federal entities	✓			ATR users will share ATR IDMS-C information with other federal partners on a case-by-case basis in accordance with organizational rules.
State, local, tribal gov't entities	✓			ATR users will share ATR IDMS-C information with others on a case-by-case basis via email in accordance with organizational rules.
Public	✓			Certain information will become public in litigation according to civil procedure, evidence, and court rules, and court orders.

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	✓	✓		ATR will share case documents with the parties and court as required by discovery rules or court orders.
Private sector	✓			ATR will share information with private sector individuals who have been hired as experts or have other legitimate reasons for access, upon approval of the case manager or other appropriate ATR authorities. ATR generally, will provide access to data via email upon case manager approval.
Foreign governments				
Foreign entities	✓			While rare, ATR may share information from ATR IDMS-C on a case by case basis with foreign entities or partners who have legitimate reasons for access and upon approval of the case manager and appropriate DOJ/ATR authorities. ATR generally will provide data via email upon case manager approval.
Other (specify):	✓		✓	A third-party application within ATR IDMS-C enables an approved ATR administrator to conduct automated searches of ATR IDMS-C for records.

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.

Any data that resides in ATR IDMS-C is processed and accessed in accordance with legal requirements, federal regulations, and Department policy. ATR provides only statistics and case filings to the "Open Data" site (www.data.gov).

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.

An ATR SORN provides generalized notice to the public.

ATR-006, "Antitrust Management Information System (AMIS) - Monthly Report," 63 Fed. Reg. 8659 (2-20-1998), 66 Fed. Reg. 8425 (1-31-2001), 66 Fed. Reg. 17200 (3-29-2001), 82 FR 24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.88.

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.

All information within ATR IDMS-C is generally second sourced and is captured, organized, and managed by individual users. Individuals involved in investigations and litigations are properly notified in accordance with Federal criminal and civil procedure and court rules. All information collected is part of existing or requested case data, as captured or requested through voluntary requests, subpoenas, discovery requests, search warrants, civil investigative demands, or second requests under the Hart-Scott-Rodino Antitrust Improvement Act ("HSR" Act).[2] For compulsory data-gathering mechanisms, individuals do not have the opportunity to decline to provide the requested data and documents. Certain information may be provided voluntarily by the data subject.[3] As required by law, ATR provides data subjects with appropriate notice of information collection under the Privacy Act, 5 U.S.C. § 552a(e)(3), e.g., when individuals submit applications for employment. Notice is not provided to individuals for information collected from public sources, because that information is publicly available.

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.

ATR follows Department procedures regarding requests for access to, or amendment of, records pertaining to an individual, including those maintained within a system of records in accordance with the Privacy Act. See https://www.justice.gov/opcl/doj-privacy-act-requests. Privacy Act requests for access to records are processed under both the Privacy Act and the Freedom of Information Act (FOIA), 5 U.S.C. § 552. All such requests are submitted to ATR's FOIA/Privacy Act Unit (https://www.justice.gov/atr/antitrust-foia) for processing and response.

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).

---

[2] The HSR Act, 15 U.S.C. § 18a, requires parties to certain transactions to notify ATR and the Federal Trade Commission of the transaction and to provide certain documents, and it permits the agencies to make a request for additional information and documents (a "second request").

[3] This type of information includes interviews of witnesses that are conducted on a voluntary basis (as compared to depositions, for example) and summarized in memos. It also includes memos to HR Managers capturing information obtained during job interviews.

	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): January 17, 2024 **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:**
✓	There are no POA&Ms associated with Privacy Controls.
	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:
	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: ATR IDMS-C is categorized as a moderate system based on a review of the aggregate impact levels for confidentiality, integrity, and availability.
	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:
✓	IDMS-C has completed all required security and functional testing and evaluation in accordance with Department IT development procedures. Additionally, the system has undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook. The system operates within the boundary of ATR CCE, where it is subject to full system monitoring and auditing in accordance with ATR and Department guidelines. All system documentation supporting these activities are maintained within the Department's system of record, Joint Cybersecurity Authorization and Management (JCAM) application.
	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:
✓	IDMS-C audits at multiple layers, including the network and application processing levels. All logs are generally reviewed on a weekly basis by onsite administrators and then gathered and centrally managed using the Department's audit analysis solution, SPLUNK. All logs are forwarded to the DOJ Security Operations Center (JSOC) for automated analysis and review.
✓	**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 IDMS-C are required to sign the DOJ General and 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:** All IDMS-C users are subject to organizational and Department annual computer security awareness and privacy specific training that includes sign off and acknowledgment of the DOJ General and Privileged Rules of Behavior. In addition, all ATR users are required to undergo formal onboarding training that includes IDMS-C specific training.

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 ATR IDMS-C users are required to undergo training and sign formal Rules of Behavior prior to being granted access to data within ATR IDMS-C. All users are required to use multi-factor authentication or unique usernames and passwords to access their ATR IDMS-C accounts. ATR IDMS-C uses CCE active directory services to support a single sign-on solution for all ATR IDMS-C accounts.

All data is encrypted at rest and during transmission outside ATR's secure boundary. Data access is restrictive; users require formal approval and authorization to access information on a case-by-case basis for data they do not own. Users can access only data which they own or are authorized by the data owner to access. Additionally, users manage their own data within ATR IDMS-C and can only grant to other users access to the data they own and control.

In addition, case data is through the use of Access Control Lists that require approval by specific data owners for granting of user access. Finally, access and audit logs are maintained within the system and are reviewed by administrators as required by DOJ policies for unauthorized access and other security and performance related concerns.

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.)

Individual users are responsible for ensuring that records processed or disseminated through ATR IDMS-C are appropriately retained or destroyed. Requirements governing retention and disposition of ATR documents and information are documented within ATR Directive 2710.1: Procedures for Handling Division Documents and Information, consistent with National Archives and Records Administration regulations and rules,

including records schedules.

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:

ATR-006, "Antitrust Management Information System (AMIS) - Monthly Report," 63 Fed. Reg. 8659 (2-20-1998), 66 Fed. Reg. 8425 (1-31-2001), 66 Fed. Reg. 17200 (3-29-2001), 82 FR 24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(k)(2). See 28 C.F.R. § 16.88.

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?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

ATR uses ATR IDMS-C as an internal document management repository. The privacy risks associated with information collected within ATR IDMS-C primarily relate to the loss of confidentiality and integrity of the data. Access by unauthorized entities to sensitive data, including personal information collected for internal personnel management use, investigation, or litigation potentially could lead to destruction or corruption of that data, compromised identities, exposure of sensitive court records and personal data, and/or disruption to an ongoing investigation or litigation.

To mitigate this risk, only authorized ATR users can access ATR IDMS-C and individual document access is further limited by Access Control Lists which are implemented and

maintained by each data owner. Additionally, ATR uses a number of proven protection methods, including secure communications through DOJ's Justice Unified Network (JUTNET), malicious code protection and intrusion detection software, active monitoring controls, encryption, and enhanced access control techniques to ensure data is protected in accordance with DOJ IT security standards and applicable U.S. Government standards. Additionally, EOS uses a specific script to audit and review access to specific data within ATR IDMS-C records.

The types of information collected within ATR IDMS-C vary greatly based on the data owner's needs. To mitigate the risk of overcollection, information collected is limited to what is necessary for each specific matter. ATR also complies with applicable record retention schedules and guidance, to prevent the storage of records within ATR IDMS-C for longer than is necessary. Finally, ATR provides user training to users of ATR IDMS-C to mitigate the risk of overcollection.

ATR IDMS-C does contain SSNs captured in support of employee payroll processing and for other human resources purposes to comply with National Finance Center, Office of Personnel Management, and other human resources law and regulatory requirements. To mitigate the risk posed by the processing of SSNs, access to SSNs is limited to HR personnel and all documents containing SSNs are controlled through access control lists and user permissions. Documents containing SSNs are also secured using encryption (sending external via email).