Antitrust Division

Privacy Impact Assessment
for the
ATR Litigation Support Systems- Cloud
ATR LSS-C

Issued by:
[Sarah Oldfield
ATR Senior Component Official for Privacy)]

Approved by: Michelle Ramsden
Senior Counsel
U.S. Department of Justice

Date approved: May 22, 2025

[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

The Antitrust Division (ATR) Litigation Support System-Cloud (LSS-C) system includes the Relativity Database Management System-Cloud (RDMS-C) and the iPRO Database Management System-Cloud (IPDMS-C) systems which ATR uses to process, analyze, manage, maintain and produce large volumes of data in connection with ATR's litigation and investigation functions. The LSS-C infrastructure is managed by ATR's Technology Directorate personnel, and the applications within the LSS-C are supported by ATR's Litigation Support Section personnel.

ATR conducts civil investigations, affirmative civil litigation, grand jury investigations, and criminal prosecutions. ATR collects documents, data, and testimony from subjects, targets, opposing parties and third parties through issuance of civil investigative demands, search warrants, civil and grand jury subpoenas, and discovery requests. ATR LSS-C stores and maintains data associated with ATR litigation, investigations, trials, international cooperation, employment matters, FOIA requests, and policies. Therefore, almost any category of PII might be implicated in this system. Employment matters and litigation or investigations involving government procurement may contain personally identifiable information (PII) about DOJ or other federal employees.

This PIA is being conducted in conjunction with a new Authorization to Operate (ATO) boundary comprised of two systems with current ATO's. ATR LSS-C is a new ATO boundary that is consolidating ATR RDMS-C, a system with a current ATO, with ATR IPDMS-C, a system without a current ATO. This consolidation allows for better administrative management of the two systems meeting ATR's criteria for like system consolidation. A PIA is required because LSS-C implicates information in identifiable form about members of the public. The existing PIAs covering RDMS-C and IPDMS-C do not cover the use of AI in RDMS-C.

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.

RDMS-C is a cloud-based Document Review Platform, with case management capabilities. It provides users features for case assessment, fact management, search, review, production, analytics, and legal holds. RDMS-C is built upon the Relativity version 2023 software deployed in the ATR instance of Microsoft Azure Government Cloud Infrastructure as a Service (ATR Azure IaaS). All data is stored in encrypted form. Users utilize hardware and

software deployed within ATR's on-premises enterprise infrastructure to access the RDMS-C system in ATR Azure IaaS.

RDMS-C uses artificial intelligence to quickly determine relevancy and privilege of document sets, protect data privacy by quickly identifying patterns that are likely to be PII, recognize sentiments in text and detect foreign language in text (although it does not provide a translation) to aid in investigations. This will help to decrease time to review large document sets.

There are limited risks associated with this AI use case. PII will be intermingled in the data sets, which could pose privacy or confidentiality concerns in the case of a data breach. As affirmed by the DOJ Emerging Technology Board and Chief AI Officer in December 2023, the use case poses minimal risks to rights or safety. Outputs will be subject to multiple levels of human legal review prior to any action being taken, which further minimizes the impact of any potential risks posed by the technology.

All data used in AI models comes from material housed in the case itself within RDMS-C. The tool does not rely on external information. The outputs of the RDMS-C AI processes and tools will be a smaller subset of documents from which document reviewers will perform further substantive analysis. This subset can be produced through training materials that are fed into a model from a set of previously reviewed and tagged data in the case. Other types of outputs from RDMS-C include finding similar documents from analyzed text, comparison of hash values to remove duplicates, identification of foreign language in text, clustering data with similar concepts or ideas together based on shared characteristics, and categorizing documents by domain, names, dates, etc.

A statistical subset of non-responsive materials is reviewed to confirm that no additional training is needed. If additional training data is needed because positive results were found in the non-responsive set, a new model, including the responsive documents is rerun and further validation testing is conducted until the statistical sample reviewed contains only non-responsive data. For other areas detected, human review will be used to ensure the analysis supplied by the platform is accurate. All of the AI's output will be reviewed by a human prior to decisions or actions to ensure accuracy, and if needed, retrain the model.

RDMS-C manages user authorizations, so personnel have access only to their approved assigned matters in RDMS-C to conduct discretionary views, searches, and sorting activities of data through artifacts to analyze documents and data to determine which are sensitive or otherwise relevant to a case. RDMS-C user types include both general and privileged internal DOJ Federal and contractor personnel, as well as external Federal Government and State officials, US vendors and expert witnesses, and a small subset of foreign expert witnesses and officials, all with strictly controlled general user access to specific resources and limited data sets. Data is retained as long as the matter remains open, or until existing document holds are released and may only be deleted by ATR Internal System Administrators. Copies of data in ATR LSS-C may be produced to the court or opposing counsel in litigation.

IPDMS-C is a cloud-based document processing and case management database system used and supported by the ATR Litigation Support Section. IPDMS-C does not store data within the

system and is only used to develop case litigation or investigative data sets which are then encrypted and exported to the ATR RDMS-C within the same environment to be used for the purposes described above. IPDMS-C is built upon the iPro Version 10 software deployed in the ATR Azure IaaS. Users utilize hardware and software deployed within ATR's on-premises enterprise infrastructure to access the IPDMS-C system in ATR Azure IaaS.

IPDMS-C manages user authorizations, so approved personnel have access to assigned matters to conduct processing, management, and manipulation of case litigation and investigative data. Only ATR Federal Employees and Full-Time on Staff Contractors are authorized accounts for IPDMS-C. Accounts are managed by the Litigation Support Staff System Administrator for IPDMS-C.

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	
Executive Order	
Federal regulation	The Antitrust Division has authority for the project under 28 C.F.R. §§ 0.40, General functions, and 0.41, Special functions
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 of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Date of birth or age	X	A, B, C, & D	Date of birth or age of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Place of birth	X	A, B, C, & D	Place of birth of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Sex	X	A, B, C, & D	The sex of DOJ or other Federal government personnel or members of the public, may be included in video surveillance, body cam footage, or other seized video material that is associated with a specific case.
Race, ethnicity, or citizenship	X	A, B, C, & D	Race, ethnicity, or citizenship information of DOJ or other Federal government personnel or members of the public, may be included in video surveillance, body cam footage, or other seized video material that is associated with a specific case.
Religion	X	A, B, C, & D	Religion information of DOJ or other Federal government personnel or members of the public, may be included in video surveillance, body cam footage, or other seized video material that is associated with a specific case.
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, & D	SSNs of DOJ or other Federal government personnel or members of the public are not collected or requested, but documents containing full or partial SSNs may be produced in investigations or litigation.
Tax Identification Number (TIN)	X	A, B, C, & D	Tax identification numbers of DOJ or other Federal government personnel or members of the public are not actively collected or requested but may be produced in investigations or litigation.

(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	A, B, C, & D	Driver's license data of DOJ or other Federal government personnel or members of the public is not actively collected or requested but may be produced in investigations or litigation.
Alien registration number	X	A, B, C, & D	Alien registration numbers of DOJ or other Federal government personnel or members of the public are not actively collected or requested but may be produced in investigations or litigation.
Passport number	X	A, B, C, & D	Passport numbers of DOJ or other Federal government personnel or members of the public are not actively collected or requested but may be produced in investigations or litigation.
Mother's maiden name	X	A, B, C, & D	Mother's maiden name information of DOJ or other Federal government personnel or members of the public is not actively collected or request but may be produced in investigations or litigation.
Vehicle identifiers	X	A, B, C, & D	License plate numbers of DOJ or other Federal government personnel or members of the public may be detected in video footage provided during investigations or surveillance.
Personal mailing address	X	A, B, C, & D	Personal mailing address information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Personal e-mail address	X	A, B, C, & D	Personal e-mail address information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Personal phone number	X	A, B, C, & D	Personal phone number information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Medical records number	X	A, B, C, & D	Medical records number information of DOJ or other Federal government personnel or members of the public may be produced in investigations or litigation.

(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
Medical notes or other medical or health information	X	A, B, C, & D	Medical notes or other medical or health information of DOJ or other Federal government personnel or members of the public may be produced in investigations or litigation.
Financial account information	X	A, B, C, & D	Financial account information of DOJ or other Federal government personnel or members of the public is collected or requested in association with a specific litigation or investigation.
Applicant information	X	A, B, C, & D	Applicant information of DOJ or other Federal government personnel or members of the public is collected or requested in association with a specific litigation or investigation.
Education records	X	A & B	Education information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Military status or other information	X	A, B, C, & D	Military status or other information of DOJ or other Federal government personnel or members of the public, may be included in video surveillance, body cam footage, or other seized video material that is associated with a specific case.
Employment status, history, or similar information	X	A, B, C, & D	Employment information of DOJ or other Federal government personnel or members of the public is collected or requested in association with a specific litigation or investigation.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, & D	Employment information of DOJ or other Federal government personnel or members of the public is collected or requested in association with a specific litigation or investigation.
Certificates	X	A, B, C, & D	Certificates information of DOJ or other Federal government personnel or members of the public is collected or requested in association with a specific litigation or investigation.

(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
Legal documents	X	A, B, C, & D	Criminal records or civil law enforcement information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation. Information related to or compiled for grand jury, criminal prosecution, or civil litigation of DOJ or other Federal government personnel or members of the public may be processed and stored in relation to a specific litigation or investigation.
Device identifiers, e.g., mobile devices	X	A, B, C, & D	Mobile device information may be collected as part of a specific litigation or investigation
Web uniform resource locator(s)	X	A, B, C, & D	Web uniform resource locator(s) information may be collected as part of a specific litigation or investigation.
Foreign activities	X	A, B, C, & D	Foreign activities information of DOJ or other Federal government personnel or members of the public may be collected as part of a specific litigation or investigation.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, & D	Criminal records information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Juvenile criminal records information	X	A, B, C, & D	Juvenile criminal records or civil law enforcement information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, & D	Civil law enforcement information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, & D	Whistleblower, e.g., tip, complaint, or referral information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.

(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
Grand jury information	X	A, B, C, & D	Information related to or compiled for grand jury, criminal prosecution, or civil litigation of DOJ or other Federal government personnel or members of the public may be processed and stored in relation to a specific litigation or investigation.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, & D	Information concerning witnesses to criminal matters, e.g., witness statements, and witness contact information of DOJ or other Federal government personnel or members of the public may be processed and stored in relation to a specific litigation or investigation.
Procurement/contracting records	X	A, B, C, & D	Procurement/contracting records information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Proprietary or business information	X	A, B, C, & D	Proprietary or business information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, & D	Location information, including continuous or intermittent location tracking capabilities information of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
Biometric data:	X	A, B, C, & D	Biometric data of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
- **Photographs or photographic identifiers**	X	A, B, C, & D	Photos, videos, or voice recordings (including video surveillance, body cam footage, or other seized video material) of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.

(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
- **Video containing biometric data**	X	A, B, C, & D	Photos, videos, or voice recordings (including video surveillance, body cam footage, or other seized video material) of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
- **Fingerprints**	X	A, B, C, & D	Fingerprints of DOJ or other Federal government personnel or members of the public may be included in parts of a security assessment conducted for clearance purposes and may be disclosed as part of a personnel file for federal employees or contractors.
- **Palm prints**	X	A, B, C, & D	Palm prints of DOJ or other Federal government personnel or members of the public may be included in parts of a security assessment conducted for clearance purposes and may be disclosed as part of a personnel file for federal employees or contractors.
- **Iris image**	X	A, B, C, & D	Iris image of DOJ or other Federal government personnel or members of the public may be included in parts of a security assessment conducted for clearance purposes and may be disclosed as part of a personnel file for federal employees or contractors.
- **Dental profile**	X	A, B, C, & D	Dental profile data of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
- **Voice recording/signatures**	X	A, B, C, & D	Photos, videos, or voice recordings (including video surveillance, body cam footage, or other seized video material) of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
- **Scars, marks, tattoos**	X	A, B, C, & D	Scars, marks, or tattoos data of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.

(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**	X	A, B, C, & D	Vascular scan, e.g., palm or finger vein biometric data of DOJ or other Federal government personnel or members of the public may be included in parts of a security assessment conducted for clearance purposes and may be disclosed as part of a personnel file for federal employees or contractors.
- **DNA profiles**	X	A, B, C, & D	DNA profiles data of DOJ or other Federal government personnel or members of the public may be collected in association with a specific litigation or investigation.
- **Other (specify)**	X	A, B, C, & D	Because of the varied nature of DOJ's work and because the system could conceivably include almost any type of unclassified PII, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system.
System admin/audit data:	X	A & B	ATR user access data is collected and stored. Also, privileged user access data is collected in association with the operation and management of this technology.
- **User ID**	X	A & B	ATR user access data is collected and stored. Also, privileged user access data is collected in association with the operation and management of this technology.
- **User passwords/codes**	X	A & B	ATR user access data is collected and stored. Also, privileged user access data is collected in association with the operation and management of this technology.
- **IP address**	X	A & B	ATR user access data is collected and stored. Also, privileged user access data is collected in association with the operation and management of this technology.
- **Date/time of access**	X	A & B	ATR user access data is collected and stored. Also, privileged user access data is collected in association with the operation and management of this technology.

(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
- **Queries run**	X	A & B	ATR user access data is collected and stored. Also, privileged user access data is collected in association with the operation and management of this technology.
- **Contents of files**	X	A & B	ATR user access data is collected and stored. Also, privileged user access data is collected in association with the operation and management of this technology.
Other (please list the type of info and describe as completely as possible):	X	A, B, C, & D	Because of the varied nature of DOJ's work and because the system could conceivably include almost any type of unclassified PII, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system.

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	X	Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify): Information may be received from other agencies or expert consultants via external storage media.					

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):	X		
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	X

Commercial data brokers	X				
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	ATR will share LSS-C information among ATR offices on a case-by-case basis. ATR generally will provide access to data via LSS-C account upon Section Chief/Assistant Chief approval. The requester's access is limited to only the requested data.
DOJ Components	X		X	ATR will share LSS-C information with DOJ Components on a case-by-case basis. ATR generally will provide access to data via LSS-C account upon Section Chief/Assistant Chief approval. The requester's access is limited to only the requested data.
Federal entities	X	X	X	ATR will share LSS-C information on a case-by-case basis with federal entities with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a

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.**
				LSS-C account, utilizing a GFE and/or RSA token through VPN, for direct log-in or using the Justice Enterprise File Sharing System (JEFS). The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.
State, local, tribal gov't entities	X		X	ATR will share LSS-C information on a case-by-case basis with State, local, or tribal government entities with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a LSS-C account, utilizing a GFE and/or RSA token through VPN, for direct log-in or using the Justice Enterprise File Sharing System (JEFS). The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes		X		ATR will share case documents with counsel, parties, witnesses, and courts as required by discovery rules or court orders. Such documents are often provided to opposing parties and courts in bulk, for example, thousands of documents could

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.**
				be provided and received by the parties in a discovery document production.
Private sector	X		X	ATR will share LSS-C information on a case-by-case basis with the private sector with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a LSS-C account, utilizing ATR's Remote Access Application Service, Virtual Desktop Interface, or by using Justice Enterprise File Sharing System (JEFS). The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff, or until the end of the case.
Foreign governments	X		X	ATR will share LSS-C information on a case-by-case basis with foreign governments with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a

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.**
				LSS-C account, utilizing a GFE and/or RSA token through VPN, for direct log-in. The requester's access is limited to only the requested data. Foreign governments with read access to ATR LSS-C are litigating partners in criminal or civil matters. The requester's access is maintained until termination is directed by the legal staff.
Foreign entities	X		X	ATR will share LSS-C information on a case-by-case basis with foreign entities such as expert witnesses with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Foreign entities must be cleared by ATR Security prior to access, after which ATR will provide training and grant access to approved/requested data via a LSS-C account, utilizing a GFE and/or RSA token through VPN, for direct log-in. The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff.
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.

ATR does not release to the public data or documents submitted by parties in investigations and litigation and stored in LSS-C. 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.

Individuals involved in investigations and litigation are properly notified in accordance with Federal criminal and civil procedures and court rules. ATR obtains most of the information stored in LSS-C through subpoenas, discovery requests, search warrants, civil investigative demands, or second requests under the Hart-Scott-Rodino Antitrust Improvements Act ("HSR" Act). For these information-gathering mechanisms, individuals do not have the opportunity to decline to provide the requested information and documents. Certain information in LSS-C may be provided voluntarily. For information collected from public sources, notice is not provided to 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.

ATR's Privacy Program Plan captures policy and procedures to ensure compliance with Federal and Department FOIA guidelines regarding requests for information or amendment, to the extent the information is in a system of records and no exemption exists. All such requests are submitted to the 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).

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): 11/22/2027 **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:** All ATO process and risk assessment materials, including the existence of POAMs resulting from those processes are recorded in the Joint Cybersecurity and Authorization Management (JCAM) records for LSS-C. This information is normally considered Information System Vulnerability Information and is controlled by the relevant Information System Security Officer.
	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:** ATR LSS-C is categorized as a moderate system based on a review of the aggregate impact levels for confidentiality, integrity, and availability.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** ATR LSS-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 has been fully incorporated within the ATR Cloud Computing Environment boundary, where it is subject to full system monitoring and audit in accordance with ATR and Department guidelines. All system documentation supporting these activities is maintained within the Department's system of record, Joint Cybersecurity Assessment and Management (JCAM).
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:** ATR LSS-C compiles audits at multiple layers, including the network and application processing levels. All logs are reviewed weekly 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.
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**. Pursuant to Department policy, contractors are generally required in their contracts to comply with the Privacy Act and other applicable laws. All contractors granted access to ATR LSS-C 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:** All LSS-C users are subject to onboarding training that includes computer security awareness and privacy training, which is an annual requirement thereafter. They are also required to undergo initial training for specific use of LSS-C during Entry on Duty. Additional LSS-C training is offered periodically, as needed for particular matters or users.

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 LSS-C users are required to undergo training and sign formal Rules of Behavior prior to being granted access to data within ATR LSS-C. All users are required to use multi-factor authentication or unique usernames and passwords to access their ATR LSS-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, System Administrators manage data access within ATR LSS-C and can only grant to other users' access to the data they have been cleared to access and have a need to know.

In addition, case data is access is managed using 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.)

Information is disposed of or retained in accordance with Directive ATR 2710.1, "Procedures for Handling Division Documents and Information," consistent with National Archives and Records Administration regulations and records schedules. Material submitted in investigations and litigation that are maintained in LSS-C and are not Federal records and are generally destroyed or returned to the submitting party when ATR closes a matter. Materials may be retained on completion of an investigation or case only in certain circumstances, including when the materials are exhibits, there is a pending formal FOIA or other request for the records, or the materials must be preserved under the Federal Records Act.

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.***

The privacy risks associated with information collected within LSS-C primarily relate to the loss of confidentiality, integrity, and availability of data. Access by unauthorized entities to sensitive data, including personal information collected for investigation or litigation potentially could lead to destruction of that data, compromised identities, exposure of sensitive court records and personal data, and/or disruption to an ongoing investigation or litigation. ATR uses several proven protection methods, including secure communications (e.g., JUTNET), malicious code protection and intrusion detection software, active monitoring controls, encryption, and enhanced access control techniques designed to safeguard data in accordance with DOJ IT security standards.

Additionally, all data collected within LSS-C is protected by encryption and file permissions and is viewable only by authorized individuals, who must authenticate and be given direct permission for each dataset. Some data that is deemed sensitive by the appropriate authorities may be redacted to prevent unauthorized viewing and render the information unsearchable. All user activity is monitored and audited based on user actions and accesses. LSS-C internal user

management module manages user access and only allows users the ability retrieve data based on each user authorized role and rights at the case/matter or data level. Once authorized, users can retrieve data by searching the LSS-C database files using a variety of parameters to include name, address, case/matter number, phone, and email. To avoid over collection, data collected is limited to a specific case or investigation but can be collected from a variety of sources. This information is shared with only approved authorized users either through direct log on to LSS-C or through other secure means, such as the Justice Enterprise File Sharing System (JEFS). ATR provides privacy notices through system of records notices (SORNS), published on DOJ's system of records website (https://www.justice.gov/opcl/doj-systems-records), and PIAs. Additionally, personnel are required to take annual Cybersecurity Awareness Training (CSAT) and privacy training.

ATR shares LSS-C information on a case-by-case basis outside DOJ with legitimate reasons for access, upon approval of the case manager and the ATR Security staff. Individuals must be cleared by ATR Security prior to access via applicable personnel security requirements, after which ATR will provide training and grant access to approved/requested read data via an LSS-C account, utilizing a GFE and/or RSA token through VPN, for direct login. The requester's access is limited to only the requested data. The requester's access is maintained until termination is directed by the legal staff.

ATR complies with Department policies and processes designed to ensure the integrity of PII in active cases. Data is strictly controlled within the system so only data objects associated with a given case are loaded into that case repository with case-specific identification and object version control. ATR establishes control over information contained in LSS-C by strictly managing access controls, limiting permissions to only those cases that a user requires, and ensuring compliance with DOJ two-factor identification and authentication requirements. Further, privacy specific analysis and reporting is maintained within an authorized Joint Cybersecurity Authorization and Management (JCAM) profile. The capability to generate reports from LSS-C is controlled by permission and limited to authorized personnel in support of the ATR litigating mission.