Antitrust Division

Privacy Impact Assessment
for the
ATR SaaS Complete Discovery Source (CDS)

Issued by:
Sarah Oldfield
ATR Senior Component Official for Privacy

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

Date approved: August 27, 2025

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or 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.)

Complete Discovery Source's (CDS) CDS Convert SaaS platform facilitates the conversion of more than 35 applications and devices into a Relativity Short Messaging Format (RSMF) with 40 application-specific metadata fields that can be processed by ATR to create near-native formatted messages. CDS constantly updates its data type processing capabilities to ensure that new formats can also be included in its service. In addition to converting raw unstructured data formats, CDS can also take individual messages and reconstitute them into chat conversations. This allows ATR to take already processed data and create the near native review format that allows attorneys to more easily follow chat conversations and provides a presentation-ready format for use at trial.

ATR collects data pursuant to civil investigative demands, civil and grand jury subpoenas, discovery requests, search warrants, civil investigative demands, court orders, and second requests under the Hart-Scott-Rodino Antitrust Improvements Act ("HSR" Act).[1] Data is transferred in raw unstructured formats, or as individual message files exported from the document review system and uploaded to the Justice Enterprise File Sharing platform (JEFS) which sits in ATR's General Support System (GSS) boundary. The vendor downloads the data from JEFS and processes it using the Federal Risk and Authorization Management Program ("FedRAMP") approved CDS Convert product. The output of that process, RSMF formatted files, are then uploaded to JEFS for ATR to download and process using ATR Litigation Support Systems- Cloud (LSS-C) before it is made available to investigation/case teams in the LSS-C.

The resources from CDS used for this process have been cleared by ATR personnel security to handle this data for ATR. Raw data files received by the vendor are retained up to 15 days after delivery of the processed output and processed data is retained no longer than 60 days after final delivery. ATR then uses internal DOJ Federal and contractor personnel to process and load the data to ATR LSS-C's document review system. Data is retained in ATR LSS-C as long as the matter remains open, or until existing document holds are released. Copies of data processed through ATR SaaS CDS and maintained in LSS-C may be produced to the court or opposing counsel in litigation.

A Privacy Impact Assessment was conducted because ATR CDS implicates information in identifiable form about members of the public.

---

[1] 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").

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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.

Information processed through the ATR SaaS CDS environment is maintained in an electronic state. ATR SaaS CDS is a pass-through system that temporarily stores and processes data associated with ATR litigation and investigations according to the data retention policies in the contract. Raw images are retained for 15 days after delivery of the processed output and processed data is retained no longer than 60 days after final delivery. Any form of PII that is available through chat-based messaging services may apply depending on the investigation or case. Employment matters and litigation or investigations involving government procurement may contain information about DOJ or other federal employees if chat information is collected as part of the investigation or litigation.

ATR SaaS CDS user types include internal Federal and contractor personnel as well as external contractor personnel for handling both the input formats and the output formats. ATR will be using authorized contract support to analyze, authorize, administer, operate, and manage services, underlying infrastructure, and interconnected system components for the creation, transfer and processing of input and output files. These ATR contract personnel are privileged users who are fully authorized and cleared for full access to applicable administrative functions based on role and responsibility within the environment. They are required to take annual CSAT and privacy training and additional role-based training as privileged users.

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	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 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 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 personnel or members of the public may be collected in association with a specific litigation or investigation.
Sex	X	A, B, C, D	Sex of DOJ or other Federal government personnel or members of the public, may have been 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 and/or ethnicity, of DOJ or other Federal government personnel or members of the public, may have been included in video surveillance, body cam footage, or other seized video material that is associated with a specific case. Citizenship of DOJ or other Federal personnel or members of the public may be collected in association with a specific litigation or investigation
Religion			N/A

(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
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	It is unlikely that this information is present in chat-based formats, however, it is not impossible. SSNs 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	It is unlikely that this information is present in chat-based formats, however, it is not impossible. Other government identifiers are not actively collected or requested but may be produced in investigations or litigation.
Driver's license	X	A, B, C, D	It is unlikely that this information is present in chat-based formats, however, it is not impossible. Other government identifiers are not actively collected or requested but may be produced in investigations or litigation.
Alien registration number	X	A, B, C, D	It is unlikely that this information is present in chat-based formats, however, it is not impossible. Other government identifiers are not actively collected or requested but may be produced in investigations or litigation.
Passport number	X	A, B, C, D	It is unlikely that this information is present in chat-based formats, however, it is not impossible. Other government identifiers are not actively collected or requested but may be produced in investigations or litigation.
Mother's maiden name	X	A, B, C, D	It is unlikely that this information is present in chat-based formats, however, it is not impossible. Mother's maiden name is not actively collected or requested but may be produced in investigations or litigation.
Vehicle identifiers	X	A, B, C, D	License plate numbers may be detected in video footage provided during investigations or surveillance.
Personal mailing address	X	A, B, C, D	Personal contact information may be collected in association with a specific litigation or investigation
Personal e-mail address	X	A, B, C, D	Personal contact information 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
Personal phone number	X	A, B, C, D	Personal contact information may be collected in association with a specific litigation or investigation
Medical records number	X	A, B, C, D	Health information may be produced in investigations or litigation.
Medical notes or other medical or health information	X	A, B, C, D	Health information may be produced in investigations or litigation.
Financial account information	X	A, B, C, D	Financial information is collected or requested in association with a specific litigation or investigation.
Applicant information	X	A, B, C, D	Applicant information is collected or requested in association with a specific litigation or investigation.
Education records	X	A, B, C, D	Employment information which may contain education records is collected or requested in association with specific litigation or investigations
Military status or other information	X	A, B, C, D	Employment information which may contain military status is collected or requested in association with specific litigation or investigations
Employment status, history, or similar information	X	A, B, C, D	Employment information is collected or requested in association with specific litigation or investigations
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, D	Employment information is collected or requested in association with specific litigation or investigations
Certificates	X	A, B, C, D	Employment information which may contain certificates is collected or requested in association with specific litigation or investigations
Legal documents	X	A, B, C, D	Legal documents are collected or requested in association with specific litigation or investigations
Device identifiers, e.g., mobile devices	X	A, B, C, D	Mobile device information will be collected and used as part of a specific litigation or investigation.
Web uniform resource locator(s)	X	A, B, C, D	Web URLs are collected in association with a specific litigation or investigation.
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	Criminal records may be collected in association with a specific litigation or investigation.
Juvenile criminal records 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
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	Civil law enforcement information may be collected in association with a specific litigation or investigation.
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, D	Information related to Whistleblowers may be processed and stored in relation to a specific litigation or investigation.
Grand jury information	X	A, B, C, D	Information related to or compiled for grand juries 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 may be processed and stored in relation to a specific litigation or investigation.
Procurement/contracting records	X	A, B, C, D	Procurement and/or contracting records may be processed and stored in relation to a specific litigation or investigation.
Proprietary or business information	X	A, B, C, D	Proprietary and/or business information related to or compiled for civil law enforcement may be collected in association with a specific litigation or investigation.
Location information, including continuous or intermittent location tracking capabilities	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.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, D	Photos (including video surveillance, body cam footage, or other seized video material) may be collected in association with specific litigation or investigation.
- **Video containing biometric data**	X	A, B, C, D	Videos (including video surveillance, body cam footage, or other seized video material) may be collected in association with specific litigation or investigation.
- **Fingerprints**			N/A
- **Palm prints**			N/A
- **Iris image**			N/A
- **Dental profile**			N/A
- **Voice recording/signatures**	X	A, B, C, D	Video recordings (including video surveillance, body camera footage, or other seized video material) may be collected in association with 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
- **Scars, marks, tattoos**	X	A, B, C, D	Scars, marks or tattoos of DOJ or other Federal government personnel or members of the public, may have been included in video surveillance, body cam footage, or other seized video material that is associated with a specific case.
- **Vascular scan, e.g., palm or finger vein biometric data**			N/A
- **DNA profiles**			N/A
- **Other (specify)**			N/A
System admin/audit data:			
- **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	Passwords to external media devices may be collected and stored in association with the operation and management of the device.
- **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.
- **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.

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

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	X	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 shares information with ATR personnel on a case-by-case basis as needed to process CDS information for purposes of civil and criminal law enforcement.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X	X		Copies of data processed through ATR SaaS CDS and maintained in LSS-C may be produced to counsel, parties, or courts in litigation.
Private sector	X	X	X	ATR shares information with the vendor via JEFS on a case-by-case basis for the purpose of the vendor processing information using the CDS Convert product into RSMF formatted files for ATR.
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.

ATR does not release to the public data or documents submitted by parties in investigations and litigation and stored in ATR SaaS CDS. 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 kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, 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.

Information about individuals processed in ATR SaaS CDS is collected by ATR through subpoenas, discovery requests, search warrants, court orders, civil investigative demands, or second requests under the HSR Act. ATR is not required to provide individual notice to all whose PII is implicated.

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 much of the information processed in ATR SaaS CDS through subpoenas, discovery requests, search warrants, court orders, civil investigative demands, or second requests under the 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 ATR SaaS CDS may be provided voluntarily.[2]

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.

---

[2] For example, during the initial waiting period of an ATR investigation under the HSR Act, ATR typically requests and parties typically provide the voluntarily submission of certain information and documents.

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) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** 3-Year ATO for ATR SaaS CDS approved on April 16, 2025 **If an ATO has not been completed, but is underway, provide status or expected completion date:** See above **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:** N/A
N/A	**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 information or information 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 NIST SP 800-60 v.2 rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** The information system has been assigned a Moderate security category for confidentiality, integrity, and availability in accordance with FIPS Publication 199 and NIST SP 800-60, Rev. 1. This categorization is based on the sensitivity of the data processed, which includes personally identifiable information (PII) and other sensitive case-related records. Unauthorized disclosure, alteration, or disruption of this information could cause significant harm to individuals' privacy, hinder legal processes, and negatively impact the mission of the Department of Justice. Therefore, a Moderate impact level is appropriate to ensure adequate protection and resilience.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** ATR SaaS CDS is currently assessing all required security and functional testing in accordance with Department IT development procedures. The system is undergoing a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook and FedRAMP requirements. The system

	will be subject to full system monitoring and audit in accordance with ATR and Department guidelines. All supporting documentation is maintained within the Department's system of record, Justice 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 SaaS CDS will conduct 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.3 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 required in their contracts to comply with the Privacy Act and other applicable laws. All contractors granted access to ATR SaaS CDS 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 ATR SaaS CDS 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 CDS during Entry on Duty. Additional ATR SaaS CDS 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 SaaS CDS users are required to use multi-factor authentication or unique username and passwords to access their ATR SaaS CDS accounts. Data access is highly restrictive; users require formal approval and authorization to access information on a case-by-case basis. Users can access only data for which they are authorized. All users are required to undergo training and sign formal Rules of Behavior prior to being granted access to ATR SaaS CDS data. For sharing of data with private sector and law firms or courts, this information is provided through a bulk export of data. Prior to export, the case team reviews records to redact references to PII or other private information unless disclosure is specifically related to the litigation.

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.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

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 processed in ATR SaaS CDS and are not Federal records or that have completed their retention period are generally destroyed or returned to the submitting party when ATR closes a matter. Materials may be retained on the 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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

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,***
- ***Type of technology employed (e.g. AI/ML),***
- ***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 processed within ATR SaaS CDS 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 malicious code protection, 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 processed within ATR SaaS CDS 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 ATR SaaS CDS user activity is monitored and audited based on user actions and accesses. ATR SaaS CDS 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 ATR SaaS CDS 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 ATR SaaS CDS 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 Computer Security and Awareness Training (CSAT) and privacy training annually. ATR shares ATR SaaS CDS information on a case-by-case basis with foreign governments with legitimate reasons for access, upon approval of the case manager, lead attorney, ATR Security staff and JSOC. 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 a CDS account. The requester's access is limited to only the requested data. Foreign governments with read-only access to ATR SaaS CDS data are partners in criminal or civil matters. 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 ATR SaaS CDS 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 Justice Cybersecurity Assessment and Management (JCAM) profile. The capability to generate reports from ATR SaaS CDS is controlled by permission and limited to authorized personnel in support of the ATR litigating mission.