Antitrust Division

Privacy Impact Assessment
for the
ATR Application Management Suite (ATR AMS)

Issued by:
Sarah Oldfield
Office of the Chief Legal Advisor
Senior Component Official for Privacy

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

Date approved: April 6, 2023

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

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

The Antitrust Division Application Management Suite (ATR AMS) is a Sensitive But Unclassified system that supports the Antitrust Division (ATR) by providing an environment for applications that process, store, and transmit management, support, and historic mission-based information. ATR AMS is owned, managed, and maintained by the ATR Executive Office's Engineering and Emerging Technologies Section (EETS).

ATR AMS is a Commercial-Off-the-Shelf (COTS) client-and-server system that is the exclusive provider of several applications (ATR AMS applications). The information processed, stored, and transmitted by ATR AMS applications includes public court and administrative filings, complaints, indictments, and final judgments, as well as statements of policy and interpretations, staff manuals, guidelines, press releases, speeches, Congressional testimony, work product, and business review letters. Management and support records include names and other information about personnel who work on ATR cases, and the number of labor hours invested in these cases. In addition, ATR AMS stores a body of historic mission-based information in databases that are accessible to authorized ATR users.

This Privacy Impact Assessment (PIA) was prepared because ATR AMS 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 AMS is broadly characterized as an environment for information technology solutions that provide ATR with tools for organizing, evaluating, and efficiently managing the Division. More specifically, ATR AMS applications provide a high-level view of ATR's overall workload, resource allocations and litigation outcomes. AMS serves as an essential resource for (1) managing day-to-day investigative and administrative operations, (2) presenting and defending ATR's budget submissions, and (3) compiling statistics responsive to inquiries from oversight agencies such as the Office of Management and Budget, General Accountability Office, and Congress.

Currently, AMS is located in two Azure regions, one is the production site for all of the AMS databases, and the other supports a back-up contingency operation for all of the AMS databases.

ATR AMS comprises approximately 35 applications (see Appendix, Table 1), that store information in automated databases and are designed to facilitate the effective management of information about ATR's operations, including merger screening, investigations, cases, appeals, National Cooperative Research and Production Act (NCRPA) reviews, business reviews, Federal Trade Commission (FTC) clearance requests, Freedom of Information Act (FOIA) requests, information relating to expenditures, and employee human resources (HR) information.

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 and 0.41
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.

The table below shows the types of data collected by the approximately 35 applications in ATR AMS. For a list of the applications, please refer to Table 1 of the Appendix.

(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			
Date of birth or age	X	A, C, and D	A – ATR AMS contains human resources data for all employees as downloaded from the National Finance Center, which contains the date of birth for employees. This data is maintained by the HR staff and has limited controlled use. A – Date of birth of employees who have applied for an official passport are displayed in the Passport Tracking application and used by the International Section to check and track the status of passport applications. Access to the passport tracking system is limited to the employees who need to know the information. C, D – Date of birth for Red Notice parties is contained in the Oracle database.
Place of birth	X	C and D	C and D – Place of birth (citizenship country) of Red Notice parties.
Gender	X	A	A – ATR AMS contains human resource data for all employees as downloaded from the National Finance Center, including gender. This data is maintained by the HR staff and has limited controlled use.
Race, ethnicity, or citizenship	X	A	A – ATR AMS contains human resource data for all employees as downloaded from the National Finance Center, including race. This data is maintained by the HR staff and has limited controlled use.
Religion			

(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, C and D	A, C and D – Social Security Numbers are collected in full but are masked in the Oracle database. ATR AMS contains human resource data for all employees as downloaded from the National Finance Center. This data is maintained by the HR staff and has limited controlled use. A – the last four digits of Social Security Numbers of employees who have applied for an official passport are maintained and used by the International Section to check and track the status of passport applications. Access to the passport tracking system is limited to the employees who need to know the information.
Tax Identification Number (TIN)	X	C and D	C and D – Tax identification number for expert witnesses.
Driver's license			
Alien registration number			
Passport number	X	A	A – Passport numbers are stored for staff who have an official passport. Records include personal passport book or card numbers for Government employees issued a federal employee passport (red cover). ATR tracks their government and personal passport and card numbers. This data is maintained and used by the International Section.
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A	A – ATR AMS contains human resource data for all employees as downloaded from the National Finance Center. This data is maintained by the HR staff and has limited controlled use.
Personal e-mail address			

(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, C and D	A – ATR AMS contains human resource data for all employees as downloaded from the National Finance Center. This data is maintained by the HR staff and has limited controlled use. C and D – Oracle database contains emergency contact information for employees, and Attorney Point of Contact of Red Notice parties.
Medical records number			
Medical notes or other medical or health information	X	A	A – ATR AMS contains health information or records, such as disability accommodations, in human resource data. This data is maintained by HR staff and has limited controlled use.
Financial account information			
Applicant information			
Education records	X	A	A – Codes for level of education are contained in the Oracle database and used by HR staff.
Military status or other information	X	A	A – ATR AMS contains veteran's preference information in the eRoom database, which is used by HR staff in connection with hiring.
Employment status, history, or similar information	X	A	A – Active status, dates of service, and similar information is maintained by HR staff in the Oracle database.
Employment performance ratings or other performance information, e.g., performance improvement plan			ATR AMS contains human resource data for all employees as downloaded from the National Finance Center, which may include performance related information. This data is maintained by the HR staff and has limited controlled use.
Certificates			
Legal documents	X	C and D	C and D – ATR AMS is used to track all civil and criminal investigations and enforcement actions, including charging documents (e.g., complaints and indictments), appeals, and Red Notices.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			

(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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	C and D – ATR AMS is used to track all criminal enforcement actions, including charging documents (e.g., complaints and indictments), appeals, and Red Notices.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	C and D – ATR AMS is used to track all civil investigations and cases.
Whistleblower, e.g., tip, complaint, or referral	X	C and D	C and D – Complaints are contained in the Correspondence and Complaint Tracking System (CCTS).
Grand jury information	X	C and D	ATR AMS is used to track all criminal investigations and cases. Grand jury information is hidden from all but approved staff.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C and D	Witness information and interviews with witnesses are tracked and logged within the MS SQL Server database.
Procurement/contracting records	X	A	Contracting and procurement financial information is downloaded from DOJ's Unified Financial Management System (UFMS).
Proprietary or business information		C and D	Consistent with ATR's mission, ATR AMS may contain proprietary or business related information.
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**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			

(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
System admin/audit data:			
- **User ID**	X	A and B	
- **User passwords/codes**	X	A and B	Passwords are masked for auditing.
- **IP address**	X	A and B	
- **Date/time of access**	X	A and B	
- **Queries run**	X	A	Queries are run against the Oracle database for auditing.
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A and B	Federal IDs are contained within the Oracle Database. ATR AMS processes large amounts of data and thus might contain other types of PII related to ATR records not listed above.

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	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

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

Other (specify): Certain types of information may be received from parties or witnesses in investigations and litigation.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X	X	X	Authorized ATR users can share information within ATR on a case-by-case basis either from the system and in accordance with organizational rules, or using direct log-in. Bulk transfers can be performed within the Component, when required.
DOJ Components	X			Authorized ATR users can share information with other DOJ components on a case-by-case basis from the system and in accordance with organizational rules.
Federal entities	X			Authorized ATR users can share information with Federal entities on a case-by-case basis from the system and in accordance with organizational rules.
State, local, tribal gov't entities	X			Authorized ATR users can share information with State and local government entities on a case-by-case basis from the system and in accordance with organizational rules.
Public	X			Authorized ATR users can share information with the public on a case-by-case basis from the system and in accordance with organizational rules. Information could become public in litigation according to civil procedure, evidence, and court rules, and court orders.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Authorized ATR users can share information on a case-by-case basis from the system and in accordance with organizational rules.

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.**
Private sector	X			Authorized ATR users can share information with the private sector on a case-by-case basis from the system and in accordance with organizational rules.
Foreign governments	X			Authorized ATR users can share information with foreign governments on a case-by-case basis from the system and in accordance with organizational rules.
Foreign entities	X			Authorized ATR users can share information with foreign entities on a case-by-case basis from the system and in accordance with organizational rules.
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.

Data that resides in ATR AMS is processed and disseminated in accordance with legal requirements, federal regulations, and Department and ATR policy. ATR provides only statistics and case filings for "Open Data" purposes.[1] However, ATR's public case filings may properly contain PII.

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.

DOJ provides individuals with generalized notice about its collection, use, and sharing of PII through a variety of Systems of Records Notices (SORNs), and, in some instances, individualized notice pursuant to Section 552a(e)(3) of the Privacy Act. Six (6) ATR SORNs and four (4) DOJ SORNs, described in section 7.2 of this document, provide generalized notice to the public.

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

[1] For a link to ATR's datasets, see https://catalog.data.gov/dataset?publisher=Antitrust%20Division.

collection or specific uses of their information? If no opportunities, please explain why.

Individuals generally do not have the opportunity to decline the use or dissemination of their information collected in ATR AMS applications for processing and use. Information in AMS is generally collected from other systems, such as National Finance Center (NFC) data, or systems of record, such as ATR-003, "Index of Defendants in Pending and Terminated Antitrust Cases," in compliance with applicable privacy law and regulations.

Additionally, ATR users do not have the opportunity to decline the collection of information associated with using ATR AMS applications. This information consists of their IP address, the date/time of access, queries run, and the content of files accessed and reviewed. ATR users have the ability to update their contact information that is displayed on the ATR internal network ("intranet") page.

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 contains policies and procedures to ensure compliance with Federal and Department FOIA guidelines regarding requests for information or amendment. All such requests are submitted to the ATR FOIA/Privacy Act Unit (https://www.justice.gov/atr/antitrust-foia) for processing and response.

Public comments and complaints can also be voluntarily submitted, and are stored in the Oracle database within ATR AMS.

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):** May 16, 2022 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** There are no privacy-related open POA&Ms.

	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 AMS 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 AMS 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 highest sensitivity information contained on this system pursuant to the Federal Information Processing Standards (FIPS) security categorization(s), as defined in NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, is Moderate and matches the most sensitive information in the system, per the 'high water mark' standard. The system operates within the boundary of ATR's cloud infrastructure environment, ATR Cloud Computing Environment (ATR CCE), where it is subject to full system monitoring and auditing in accordance with the Department of Justice guidelines. System documentation supporting these activities are maintained within the Department's system of record, Cyber Security Assessment & Management (CSAM) tool.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** ATR AMS satisfies the Audit and Accountability (AU) controls outlined by NIST 800-53A-Rev.5, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. All approved policies, procedures, standards, and program plans fully meet the requirements of FISMA.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. All contractors granted access to ATR AMS are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role. All associated IT-related contracts within ATR are required to comply with the policies and guidelines defined and documented within the Department of Justice Procurement Guidance Document 15-03, Security of Information and Information Systems.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** There is no additional privacy training specific to this system.

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?

ATR personnel, both government and contractor, sign the DOJ Rules of Behavior prior to being granted access to the ATR network, and annually thereafter as a part of the DOJ cybersecurity awareness training. ATR users are required to use multi-factor authentication, to access the ATR network. ATR AMS depends on the active directory services of the ATR General Support System (GSS) to support a single sign-on solution and to audit unauthorized access to the ATR network.

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.)

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.

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:

The SORNs listed below cover the records, within systems of records, which will be implicated by the applications within ATR AMS:

- ATR-001, "Antitrust Division Expert Witness File," 54 Fed. Reg. 42060, 061 (10-13-1989), 66 Fed. Reg. 8425 (1-31-2001), 82 Fed. Reg. 24147 (5-25-2017).
- ATR-003, "Index of Defendants in Pending and Terminated Antitrust Cases," 60 Fed. Reg. 52690 (10-10-1995), 66 Fed. Reg. 8425 (1-31-2001), 82 Fed. Reg. 24147 (5-25-2017).
- ATR-005, "Antitrust Management Information System (AMIS) - Time Reporter," 53 Fed. Reg. 40502 (10-17-1988), 66 Fed. Reg. 8425 (1-31-2001), 82 Fed. Reg. 24147 (5-25-2017).

- ATR-006, "Antitrust Management Information System (AMIS) - Matter 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.

- ATR-014, "Civil Investigative Demand (CID) Tracking System," 60 Fed. Reg. 52690, 694 (10-10-1995), 66 Fed. Reg. 8425 (1-31-2001), 82 Fed. Reg. 24147 (5-25-2017).

- DOJ-001, "Accounting Systems for the Department of Justice," 69 Fed. Reg. 31406 (6-03-2004), 71 Fed. Reg. 142 (1-3-2006), 75 Fed. Reg. 13575 (3-22-2010), 82 Fed. Reg. 24147 (5-25-2017).

- DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 64 FR 73585 (12-30-1999), 66 FR 8425 (1-31-2001), 82 FR 24147 (5-25-2017), 86 FR 37188 (7-14-2021). Exemptions claimed pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). *See* 86 FR 61687.

- DOJ-009, "Emergency Contact Systems for the Department of Justice," 69 Fed. Reg. 1762 (1-12-2004), 82 Fed. Reg. 24147 (5-25-2017).

- DOJ-014, "Department of Justice Employee Directory Systems," 74 Fed. Reg. 57194 (11-4-2009), 82 Fed. Reg. 24151, 153 (5-25-2017).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

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.***

To mitigate the risk of unauthorized access into the system, ATR establishes control over information contained in ATR AMS by strictly managing access controls. DOJ background checks are performed on all DOJ personnel, including ATR employees and contractors. In addition to

background checks, all ATR personnel are required to complete annual computer security awareness training and sign the "DOJ Cybersecurity and Privacy Rules of Behavior (ROB) for General Users" which include rules for safeguarding identifiable information. In addition, ATR AMS staff and others requiring privileged access to ATR AMS are required to sign the DOJ Privileged Rules of Behavior (PROB).

Direct access to ATR AMS is available only to authorized ATR employees, contractors and other personnel. Access to applications and data is limited by roles defined in the ATR AMS system. ATR AMS authorized users can gain access to approved applications only by using a valid Personal Identify Verification (PIV) card and/or network ID and password, including authentication through ATR mobile devices via ATR's intranet. ATR GSS supports a single sign-on solution, through the Active Directory Federated Services (ADFS). Authorized ATR users can share information within ATR, and other sources, on a case-by-case basis via emailed reports from the system and in accordance with organizational rules. SORNs provide generalized notice to the public.

To mitigate the risk of collecting inaccurate or outdated information, ATR has implemented a series of checks and balances to help ensure that only applicable and accurate information is stored in the system. The sources of information for ATR AMS are as follows:

1. Human resource data for all employees as downloaded from the National Finance Center. This data is maintained by the HR staff and has limited controlled use.
2. Financial information is downloaded from DOJ's UFMS.
3. HSR Act premerger notifications are downloaded from the FTC.
4. ATR users may input data directly into AMS applications.

To mitigate cybersecurity risks on the ATR network, security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance, and security logs are enabled to assist in troubleshooting and forensics analysis during incident investigations. In addition, 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. Finally, the system leverages FedRAMP compliant cloud service infrastructure with security controls, including physical safeguards appropriate for a FISMA "moderate" system.

ATR follows a records retention schedule and policies designed to prevent of the maintenance of data that is no longer needed to fulfill the mission. Requirements governing the 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. Finally, ATR Internet links to the Department's privacy policy at https://www.justice.gov/doj/privacy-policy to explain how PII data is used in situations where ATR collects this type of information from individuals.

Table 1
Application Management Suite (AMS)
Application Portfolio

Application Name
Appellate Docket System
Business Objects
Central Files Tracking System
Civil Practice Management System
Closed File Tracking Application
Close Civil Merger System
Confluence Wiki
Correspondence / Complaint Tracking System
Criminal Case Sentencing System
Criminal Practice Management
Document Control Number Application
EAG Working Papers
eRoom Collaborative System
Exit Survey Application
Expert Witness (OBD-47) Tracking & Business Process
FedEx Statement Tracking System
FOIA Tracking System
Google-Like Search Tool
GTA Authorization Request Form and Process Automation
Hart-Scott-Rodino Tracking System
HR Projection System
Human Resources Supplemental System
Human Resources Tracking System
Incur Litigation Expense Request and Process Automation
Judgment Tracking System
Leadership Development Survey
Matter Tracking System
New Employee Survey Application
Passport Tracking System
Purchase Card Statement Tracking System
Recruitment Tracking System for Paralegals
Time Reporting System
Trial Schedule Management System
Web Document Tracking System
Web Work Product Document Submission System