Antitrust Division

Privacy Impact Assessment
for the
ATR General Support System

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

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: March 20, 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's General Support System (ATR GSS) is a major system that provides the infrastructure that supports end-user IT service delivery. The ATR GSS is directly managed and operated by ATR personnel. The system contains hardware, including servers, personal computing equipment (laptops/desktops/tablets/mobile devices, printers, and scanners), and networking equipment (including routers, switches, and data storage devices). The system provides capabilities to organize and manipulate data used in ATR business processes through Commercial Off the Shelf (COTS) software, applications, and other productivity tools.

ATR GSS serves as the infrastructure for a number of systems, databases, and applications. These systems, databases, and applications are covered by separate Initial Privacy Assessments (IPAs) and Privacy Impact Assessments (PIAs). This ATR GSS IPA addresses only network drives and data not covered under separate major ATR system IPA/PIAs.

The network infrastructure contains a significant amount and variety of information that ATR creates, collects, maintains, and disseminates in support of its mission to promote economic competition through enforcing and providing guidance on antitrust laws and principles. Network drives consist of section drives and/or shared drives for all ATR sections, offices, and units. ATR user's personal data has been migrated to Microsoft's OneDrive. With respect to shared drives, all personnel in a particular section or office have access to that section or office's designated drive. With the appropriate authorization, personnel may also obtain access to files on the network drives of another section or office in connection with a particular assignment.

ATR conducted this Privacy Impact Assessment to document its use of GSS, in accordance with Section 208 of the E-Government Act of 2002.

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 GSS is an existing environment, replacing Office Automation System (OAS) GSS, that provides the infrastructure and support for ATR's hardware including servers, personal computing equipment, routers, switches, storage device systems, WIFI, and applications. Devices within the ATR GSS are connected via an internally managed local area network (LAN) in each ATR office location. The Department of Justice Unified Network (JUTNET)

provides Wide Area Network connectivity services for all ATR offices, and provides the ability to utilize shared services provided by JMD, to include Office 365 (Mail, Microsoft SharePoint, and Microsoft Teams), Internet, video teleconferencing, phone services, and Federated Authentication and Certificate Services. GSS provides connectivity to ATR offices in Chicago (CHI), New York (NYO), San Francisco (SFO), and the Main Justice Building (MJB), and supports remote trials nationwide. In addition, ATR GSS provides WIFI connectivity for ATR mobile devices amongst all of its offices.

The network infrastructure processes information collected, maintained, and disseminated in furtherance of ATR's mission, management, and administration. The types of information on the network drives of the civil and criminal enforcement sections includes information received pursuant to the Hart-Scott-Rodino Act,[1] Civil Investigative Demands, and subpoenas; grand jury information; video recordings and transcripts of depositions; internal memoranda; working papers and drafts; and court filings. These records may contain personally identifiable information about members of the public, including personal contact information, dates of birth, and employment histories. Other personally identifiable information may include medical or health information, tax identification numbers, or social security numbers, for example, although such information is not typically collected or received in ATR matters. The Executive Office network drives contain personally identifiable information necessary for human resources administration, including social security numbers, salary and benefit information, and performance ratings.

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

[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").

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.

GSS is not a system that actively collects PII from individuals. It serves as a system infrastructure to house data such as network drives. The table below tries to capture all possible PII that ATR personnel could store on those drives. For the row entries without comments in the fourth column, all PII mentioned in the first column could be stored in GSS.

(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	
Example: Personal email address	*X*	*B, C and D*	
Name	X	A, B, C and D	
Date of birth or age	X	A, B, C and D	
Place of birth	X	A, B, C and D	
Gender	X	A, B, C and D	
Race, ethnicity, or citizenship	X	A, B, C and D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	The last four digits of SSN's are collected for parking, and as part of the DCSA background investigation process for applicants and reinvestigation of personnel every five years, and are stored on both personal and shared network drives. There could also be full SSNs on documents (unstructured data) stored in the drives in GSS.
Tax Identification Number (TIN)	X	A, B, C and D	
Driver's license	X	A, B, C and D	
Alien registration number	X	A	
Passport number	X	A	
Mother's maiden name	X	A, B, C and D	
Vehicle identifiers	X	A, B, C and D	
Personal mailing address	X	A, B, C and D	
Personal e-mail address	X	A, B, C and D	
Personal phone number	X	A, B, C and D	
Medical records number			

(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 and D	
Financial account information	X	A, B, C and D	
Applicant information	X	A	
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B, C and D	
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	
Certificates	X	A	
Legal documents	X	A, B, C and D	
Device identifiers, e.g., mobile devices	X	A	Electronic device identifiers are contained within the Mobile Device Management (MDM) application.
Web uniform resource locator(s)	X	A, B, C and D	
Foreign activities	X	A	Downloaded documents from the Justice Enterprise File Sharing (JEFS) system reflect communication with foreign antitrust agencies that is stored on personal, or shared, network drives.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C and D	
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C and D	
Grand jury information	X	A, B, C and D	Grand jury information is on network drives, as well as a limited number of non-standard special use computers maintained and individually purposed for litigation or courtroom use.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	
Procurement/contracting records	X	C and D	
Proprietary or business information	X	A, B, C and D	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
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)**			
System admin/audit data:			
- **User ID**	X	A	User ID's are masked in audit logs.
- **User passwords/codes**	X	A	User passwords are masked in audit logs.
- **IP address**	X	A	System admin/audit data is collected via Active Directory for all users
- **Date/time of access**	X	A and B	
- **Queries run**	X	A and B	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Given of the varied nature of ATR's work GSS data 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):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	X
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): USDA (National Finance Center), OPM (Enterprise Human Resources Integration/personnel records and e-QIP)					
Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

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

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer (Zipped Files)**	**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	Information may be shared with Division personnel with a need to know the relevant information via email, shared drives, or Microsoft applications.
DOJ Components	X	X	X	Information may be shared with DOJ personnel with a need to know the relevant information via DOJ collaboration tools, email, Microsoft applications, and other covered applications.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer (Zipped Files)**	**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.**
Federal entities	X	X	X	Information may be shared with federal personnel with a need to know the relevant information via encrypted email or DOJ encryption tools, including Justice Enterprise File Sharing (JEFS).
State, local, tribal gov't entities	X	X	X	Information may be shared with state, local, tribal, or territorial governmental personnel with a need to know the relevant information via encrypted email or DOJ encryption tools, including Justice Enterprise File Sharing (JEFS).
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X	X		Information in case documents may be shared with counsel, parties, witnesses, and courts with a need to know the relevant information and will be protected in accordance with any Privacy Act or other restrictions on that information.
Private sector	X	X		While this is partially captured above, information in case documents may be shared with expert witnesses with a need to know the relevant information and will be protected in accordance with any Privacy Act or other restrictions on that information.
Foreign governments	X	X		Information, including information in case documents, may be shared with foreign government personnel with a need to know the relevant information via encrypted email or DOJ encryption tools, including Justice Enterprise File Sharing (JEFS) with waiver.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer (Zipped Files)	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.
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.

Information that resides in network or shared drives is handled and released in accordance with organizational and Department requirements. 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.

ATR SORNs provide 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.

DOJ-006, "Personnel Investigation and Security Clearance Records for the Department of Justice," 67 Fed. Reg. 59864 (9-24-2002), 69 Fed. Reg. 65224 (11-10-2004), 82 Fed. Reg. 24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(j) and (k). See 28 C.F.R. § 16.132.

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.

For compulsory data-gathering mechanisms, individuals do not have the opportunity to decline to provide the requested data and documents. Certain HR-related information may be provided voluntarily by the data subject. As required by law, ATR provides data subjects with appropriate notice of information collection under the Privacy Act, 5 U.S.C. § 552a(e)(3), e.g., when individuals submit applications for employment. Notice is not provided to individuals for

information collected from public sources, because that information is publicly available.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

ATR's Privacy Program Plan captures policies and procedures to ensure compliance with Federal and Department FOIA and Privacy Act guidelines regarding requests for information or amendment. All such requests are submitted to the Division's FOIA and 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):** October 31, 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 (POA&Ms) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POA&M 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 GSS 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 GSS has completed all required security and functional testing and evaluation in accordance with Department IT development procedures. Additionally, the system has undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook. The system operates within the boundary of ATR, and as a Component is subject to full system monitoring and

	auditing in accordance with the Department of Justice guidelines. All 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-assigned personnel provide bi-weekly auditing reports to the ISSO, and team, for review. In addition to ATR, JMD has oversight of the logs for review and action.
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 GSS are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role. ATR contract personnel are general and privileged users who are authorized for full access to all data that is processed, disseminated, disclosed, and disposed of within the environment, depending on their assigned section.
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?

User access to ATR GSS is controlled by Microsoft Active Directory. ATR users are required to use multi-factor authentication, or unique username and passwords, to access the ATR network. Active directory services support single sign-on solutions for most user account access to required applications. All other application authorization is managed by specific applications in separate system boundaries.

Active Directory prohibits unauthorized network users from authenticating to interact with ATR information. Microsoft Active Directory manages user access and only allows users the ability to retrieve data based on each user authorized role and permissions via Security Groups, Organizational Units, and Group Policy Objects. Once recognized as an authorized user, users can then interact with ATR data.

All ATR personnel are required to complete annual computer security awareness training and sign DOJ Cybersecurity and Privacy Rules of Behavior for General Users (GROB) which include rules for safeguarding identifiable information. In addition, ATR GSS personnel, and others requiring privileged access to ATR GSS and its applications and/or information systems, sign the DOJ Cybersecurity and Privacy Rules of Behavior for Privileged Users (PROB).

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 records schedules.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

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

DOJ-006, "Personnel Investigation and Security Clearance Records for the Department of Justice," 67 Fed. Reg. 59864 (9-24-2002), 69 Fed. Reg. 65224 (11-10-2004), 82 Fed. Reg. 24147 (5-25-2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(j) and (k). See 28 C.F.R. § 16.132.

Section 8: Privacy Risks and Mitigation

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

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

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

ATR establishes control over information contained in GSS by strictly managing access controls for network and shared drives, mitigating the risk of unauthorized access into the system. ATR GSS user types include general and privileged internal DOJ employees, contractors, and detailees, all with strictly controlled access to specific resources and limited data sets. ATR GSS is also physically controlled with limited access provided to authorize ATR personnel via PIV authentication. Outside expert witnesses obtain access to ATR data via DOJ Connect using an RSA Token and are only given access to information needed to support a case. Access for outside expert witnesses is controlled by Microsoft Active Directory.

Users of the network can only gain access to the data by a valid PIV card and/or user ID and password, to include authentication through ATR mobile devices. Access to data on network drives is further limited to user permissions and roles associated to their section. Users are also provided access to Microsoft's One Drive where they can store their personal files. In the event of the loss of an asset, laptops and iPhones are encrypted.

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 for all computers to assist in troubleshooting and forensics analysis during incident investigations. Information sharing occurs only when the user is granted access.

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. 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.

To mitigate the risk of oversharing sensitive information, ATR's incident response personnel, CISO, and CIO receive daily Data Loss Protection (DLP) reports from the Justice Security Operations Center (JSOC) when a user sends information to email accounts outside of DOJ. JSOC also has the ability to monitor the email contents for PII, even if the email is encrypted. DLP reports are also used to prevent transmission of SSNs outside of DOJ for privacy and cybersecurity reasons. To mitigate overcollection, GSS doesn't actively collect/store SSNs. But it does support activity/systems where individuals may store documents containing SSNs which in some cases the SSN is stored in GSS (parking) but in other cases the SSN passes through GSS to other ATR systems. SSN's are only available to certain users with a need-to-know, as approved by each section's Chief.

ATR Internet links to the Department's privacy policy at https://www.justice.gov/doj/privacy-policy.