Antitrust Division

Privacy Impact Assessment
for the
ATR Web Services System (ATR WSS)

Issued by:
Dorothy Fountain
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: February 8, 2022

(May 2019 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 ATR Web Services System (ATR WSS) supports the Antitrust Division (ATR) by maintaining and updating content for the ATR public and internal websites. The primary purpose of the ATR public websites, https://www.justice.gov/atr and https://www.justice.gov/procurement-collusion-strike-force (collectively, ATR Internet), is to provide information about ATR and the Procurement Collusion Strike Force (PCSF) to the public. ATR's internal intranet website (ATRnet) provides internal information and communication accessible only to the ATR workforce. DOJ's intranet website (DOJNet) is used to share ATR event presentation materials (including recorded video presentations) to a wider audience at DOJ, and provides section/office leadership information and links to general ATR information on the ATR Internet. In addition, ATR WSS supports day-to-day operations including search, analytics, and accessibility; and serves as an administrative and utility tool that facilitates web and litigation support functions available only to ATR employees.

ATR WSS is a combination of servers, platforms, and software used by ATR staff to support the ATR mission.[1] The ATR WSS interacts with the ATR Application Management Suite (ATR AMS) through a database and displays content on ATRnet. ATR Internet is managed through the Department's web content management system, which is hosted by appropriately secure cloud-based service provider(s). ATR WSS contains dedicated servers that host commercial and proprietary applications for web support including analytics, surveys, search functionality, media streaming, databases, file and project management, and standards compliance.

This Privacy Impact Assessment (PIA) was prepared because ATR WSS 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.

[1] ATR WSS servers were migrated from the Liberty Square Building in Washington, DC to the DOJ-ATR Azure Infrastructure as a Service (IaaS) environment in Virginia. ATR WSS is also being configured to migrate the contingency/disaster recovery/continuity of operations mirrored instance of its network servers and systems from the DOJ Core Enterprise Facility - East (CEF-E) in West Virginia to the DOJ-ATR Azure IaaS environment in Texas.

ATR WSS acts as a framework from which data, documents, and applications from other systems can be viewed. A wide range of information is stored in and/or linked to other ATR information systems. For example, ATR directives posted on ATRnet are also stored in iManage to preserve the version history. The other systems linked to WSS have their own Initial Privacy Assessments (IPAs) and/or PIAs.

ATR Internet content includes ATR press releases, speeches, articles, case filings, guidelines and policy statements. It also provides ATR contact information for members of the public who wish to contact ATR by email, physical mail, or phone. At times, ATR Internet provides information regarding events that may include an ATR e-mail address or form for individuals to register. It also provides a web-based feedback form (https://www.justice.gov/atr/webform/website-comments-and-suggestions-0) through which individuals can submit comments and suggestions about the website. The comments-and-suggestions page includes optional fields for individuals to provide their names or email addresses. In addition, members of the public may submit information regarding potential antitrust violations affecting government procurement through the Procurement Collusion Strike Force (PCSF) Tip Center online web form (https://www.justice.gov/atr/pcsf-citizen-complaint) that requests specific information—for example, who was involved, what was affected, what happened, and contact information—but the form can be filled out and submitted anonymously. If supplied, contact information consists of first name, last name, street address, city, state, zip code, phone number, and email address.

ATRnet content includes ATR announcements, notices of training and other events, antitrust news, press releases, links to web tools, personnel contact information, and ATR directives and guidance. ATR's site on DOJNet is the portion of the JMD hosted website that displays certain ATR information for all DOJ employees. ATR's site on DOJNet links to the ATR Internet, including the PCSF website through which DOJ employees can submit tips to ATR. ATR also shares ATR event presentations on DOJNet.

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	This project is authorized under the Antitrust Division's statutory jurisdictional authorities, which are discussed in Chapter II of the Antitrust Division Manual, Fifth Edition, available at https://www.justice.gov/atr/file/761166/download. The E-Government Act of 2002 (https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf) authorizes the dissemination of agency information on the Internet.
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of	

	understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	Names posted on ATRnet are taken from the ATR Personnel Directory and ATR AMS. Names also appear in content submitted for publication on the websites. The PCSF web form requests, but does not require, that members of the public submit their names. ATR Internet also provides a page for members of the public to submit comments or suggestions regarding the website. This page has optional first and last name fields. Names also appear on the ATR Internet in contact information for ATR leadership, case filings, press releases, and events.
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship	X	A	ATRnet displays component specific employee workforce diversity statistics provided by DOJNet for transparency into agency hiring practices
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)			
Tax Identification Number (TIN)	X	C and D	Redacted (full or partial) tax identification numbers of individuals may appear in case filings or exhibits accessible on ATRnet and/or the ATR Internet.
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	B, C and D	The PCSF web form requests, but does not require, that members of the public submit their street address. (https://www.justice.gov/atr/webform/pcsf-citizencomplaint) A personal mailing address may be received in a public comment, case, event registration, or initiative.

(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 e-mail address	X	B, C and D	The PCSF web form requests, but does not require, that members of the public submit their email address. (https://www.justice.gov/atr/webform/pcsf-citizencomplaint) ATR Internet also provides a page for members of the public to submit comments or suggestions regarding the website. This page has an optional email address field (https://www.justice.gov/atr/webform/websitecomments-and-suggestions-) A personal e-mail address may be received in a public comment, case, event registration, or initiative.
Personal phone number	X	B, C and D	The PCSF web form requests, but does not require, that members of the public submit their phone number. (https://www.justice.gov/atr/webform/pcsf-citizencomplaint) A personal phone number may be received in a public comment, case, event registration, or initiative.
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	C and D	Event registrants may submit reasonable accommodation requests when registering for an event on ATR Internet. But this health information is only shared with those who need-to-know the information, e.g., to provide the accommodation requested.
Financial account information			
Applicant information			
Education records			
Military status or other information	X	B, C and D	ATR websites may display military status in biographies, curricula vitae or case filings.
Employment status, history, or similar information	X	A	Curricula vitae are listed on both ATRnet and ATR Internet. "Welcome to the Division" announcements are listed on ATRnet with employment status and history. Biographical information is detailed on ATR Internet for Front Office Leadership. The PCSF web form requests, but does not require, employment information.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Legal documents	X	C and D	The websites make accessible ATR's civil complaints and criminal indictments and informations alleging violations of the antitrust and related laws; key case filings; and press releases describing arrests, indictments, and lawsuits filed by ATR.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities	X	A, B, C and D	Speeches, international agreements, and press releases are listed on ATRnet and ATR Internet.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	Case filings and press releases are listed on ATRnet and ATR Internet.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C and D	Case filings and press releases are listed on ATRnet and ATR Internet.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C and D	Redacted leniency letters are accessible on ATR Internet. The PCSF form collects complaints and tips submitted by the public. "Report Violations" page on ATR Internet may collect PII.
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact 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
Procurement/contracting records	X	A, B, C and D	Procurement information may be contained in case documents on ATRnet or ATR Internet.
Proprietary or business information	X	A, B, C and D	Civil and criminal case documents may contain business information on ATRnet or ATR Internet.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C and D	ATR Internet contains photographs of ATR activities that show ATR personnel and potentially other individuals, e.g., speeches and events.
- **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	ATR WSS captures DOJ User ID's for its applications.
- **User passwords/codes**	X	A	ATR WSS user passwords/codes are masked in the logs

(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
- **IP address**	X	A, B, C and D	Logs could collect user IP addresses and general browser and operating system information, duration of session, and pages viewed from users who access ATRnet and ATR Internet. However, the log files will not contain distinct information that directly links this data back to a specific user.
- **Date/time of access**	X	A, B, C and D	Both ATRnet and ATR Internet collect this information. However, the log files will not contain distinct information that directly links this data back to a specific user.
- **Queries run**			
- **Content of files accessed/reviewed**	X	A, B, C and D	Both ATRnet and ATR Internet collect this information. However, the log files will not contain distinct information that directly links this data back to a specific user.
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Attorney bar numbers may be listed on case filings available on ATRnet and ATR Internet. Additionally, ATR's various web forms may collect, although the forms do not request, personal information not covered by one of the categories, 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	√	Hard copy: mail/fax	√	Online	√
Phone	√	Email	√		
Other (specify):					

Government sources:					
Within the Component	√	Other DOJ Components	√	Online	√
State, local, tribal	√	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	√		
Other (specify): For copies of international agreements: https://www.justice.gov/atr/antitrust-cooperation-agreements.					

Non-government sources:					
Members of the public	√	Public media, Internet	√	Private sector	√
Commercial data brokers	√				
Other (specify): Staff are re-directed to non-governmental sources from the ATR and DOJ online libraries.					

Section 4: Information Sharing

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

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	√		√	ATR personnel can view ATRnet and download various documents, as needed. Select ATR staff in designated groups can access specialized, or restricted content.

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.**
DOJ Components	√			ATR will share information with other DOJ components on a case-by-case basis. DOJ employees outside of ATR have limited access to DOJNet and ATR Internet only.
Federal entities	√		√	ATR will share information with other Federal entities on a case-by-case basis from ATR Internet, ATRnet and DOJNet if given access to the ATR network.
State, local, tribal gov't entities	√		√	ATR will share information with state, local, and tribal government entities on a case-by-case basis from ATR Internet, ATRnet and DOJNet if given access to the ATR network.
Public	√			These individuals only have access to publicly available information on the ATR Internet.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	√			These individuals have access to information related to or used in litigation, and otherwise, only have access to publicly available information on the ATR Internet.
Private sector	√			Private sector only has access to publicly available information on the ATR Internet.
Foreign governments	√			Foreign governments only have access to publicly available information on the ATR Internet.
Foreign entities	√			Foreign entities only have access to publicly available information on the ATR Internet.
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.

Certain public information available on ATR Internet is also available through data.gov. Datasets include Ten Year Workload Statistics, Sherman Act Violations Yielding a Corporate Fine of $10 Million or More, and Select Case Filings. Information is shared by posting on ATR Internet and by updating related metadata in the DOJ online catalog that is interconnected with data.gov.

In addition, metadata regarding ATR's Economic Analysis Group Working Papers is provided to RePEc (Research Papers in Economics) (http://repec.org) with links back to content on the ATR

Internet.

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.

Two 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.

ATR-009, "Public Complaints and Inquiries File," 45 Fed. Reg. 57898, 902 (11-17-1980); 66 Fed. Reg. 8425 (1-31-2001); 82 Fed. Reg. 24147 (5-25-2017).

Additionally, the Department provides a privacy policy (https://www.justice.gov/doj/privacy-policy) which is displayed on the ATR Internet. Finally, the PCSF web form contains a Privacy Act § 552a(e)(3) notice for individuals.

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.

Public comments received in connection with civil antitrust settlements are included in case filings that are available on ATR Internet and ATRnet. Other public comments available on the website include those received in response to solicitations for events (such as workshops, hearings, and general requests for public input) and proposed policy changes. Comments are voluntary and submitters are informed that comments will be made public.

Individuals are informed on the PCSF web form that their disclosure of information is voluntary. By submitting the completed form, individuals consent to ATR's collection and specific uses of their information.

Individuals do not have the opportunity to decline the collection of information in connection with them visiting the ATR Internet. While names are not collected when individuals visit at ATR websites, information that is automatically collected consists of their IP address, the date/time of access, queries run, and the content of files accessed. These data points are captured in DOJ JMD IT audit log files.

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 Privacy Act and FOIA guidelines regarding requests for information or amendment, to the extent no exemption exists, and as to the Privacy Act, to the extent the information is in a system of records. All such requests are submitted to the ATR FOIA/Privacy Act Unit (https://www.justice.gov/atr/antitrust-foia) for processing and response.

With regards to public comments, members of the public are informed that their comments may be posted on ATR Internet. A contact is also provided on the website in case individuals would like to request correction of their information and the case or event coordination staff will consider all requests.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** 11/17/2021 **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:** None
	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:
	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:
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 WSS satisfies the Audit and Accountability (AU) controls outlined by NIST 800-53A-Rev. 4, 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**.

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-related 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, 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, or unique usernames and passwords, to access the ATR network, to include the ATRnet. ATR WSS depends on the active directory services of the ATR General Support System (GSS) to support a single sign-on solution for ATRnet.

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 (NARA) regulations and rules, including requirements for ATR staff to submit documents for posting on ATRnet and ATR Intranet.

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.

ATR-009, "Public Complaints and Inquiries File," 45 Fed. Reg. 57898, 902 (11-17-1980); 66

Fed. Reg. 8425 (1-31-2001); 82 Fed. Reg. 24147 (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.***

ATR establishes control over information contained in WSS by strictly managing access controls for individual applications, mitigating the risk of unauthorized access into the system. First, a DOJ background check is performed on all DOJ personnel, including ATR employees and contractors. All ATR personnel are also required to complete annual computer security awareness training and sign "DOJ Cybersecurity and Privacy Rules of Behavior (ROB) for General Users" which include rules for safeguarding identifiable information before gaining access to the system. In addition, ATR Web Services Section personnel, and others requiring privileged access to ATR WSS, sign the DOJ Privileged Rules of Behavior (PROB).

Direct access to ATRnet is available to ATR employees, as well as contractors and other authorized personnel. ATRnet users can gain access to the data only by a valid PIV card and/or user ID and password, to include authentication through ATR mobile devices. ATR GSS supports a single sign-on solution for ATRnet. Access to some data in the system is further limited by the user's assigned role within the system, for example, to update personal contact information or certain matter information.

To mitigate cybersecurity risks on the ATR network, security personnel conduct monthly 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. 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. In addition, the system leverages FedRAMP compliant cloud service infrastructure with security controls, including physical safeguards appropriate for a FISMA moderate system.

To mitigate overcollection in the PCSF web form, the form's text fields limit the number of characters that can be entered.

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 NARA regulations and rules. The directive also governs the submission of documents to ATR WSS staff for posting on ATRnet (internal to ATR only) and ATR Internet (public website). Content with privacy concerns is removed or redacted as appropriate. ATR Internet links to the Department's privacy policy at https://www.justice.gov/doj/privacy-policy. Additionally, the PCSF web form contains a Privacy Act § 552a(e)(3) notice for individuals.

To mitigate the risk of overpublishing sensitive information, ATR has implemented series of checks and balances to ensure that only approved information is publicly distributed. ATR's Office of Operations has several layers of reviews to ensure that all content and metadata is accurately published. ATR also uses various distinct technologies to distribute information to the public:

- ATR uses Gov Delivery to send specific sets of information, such as press releases, to subscribed users.
- ATR uses Twitter (https://twitter.com/privacy?lang=en), Eventbrite (https://www.eventbrite.com/support/articles/en_US/Troubleshooting/eventbriteprivacy-policy?lg=en_US), and the Department's YouTube channel (https://policies.google.com/privacy) to communicate with the broader public.
- To provide a better user experience, ATR also uses Siteimprove (https://siteimprove.com/en/privacy/) and Archive Social (https://archivesocial.com/privacy/). Siteimprove provides section 508 services while Archive Social keeps track of all activity on the websites via log files.

The Division's use of these tools is covered under the existing DOJ PIA, Use of Third-Party Social Media Tools to Communicate with the Public (https://www.justice.gov/Use_Third_Part_Social_Media_Tools/download).