Antitrust Division

Privacy Impact Assessment
for the
Antitrust Division
Physical Access Control System (ATR PACS)

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: July 30, 2021

(May 2019 DOJ PIA Template)

(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
- **User passwords/codes**	X	A	All administrators use unique passwords and PIV cards
- **IP address**	X	A	IP address information is contained within the system
- **Date/time of access**	X	A, B, C, D	Access logs with date and time of access are maintained within the system and are generally limited to the user and administrators
- **Queries run**	X	A	Query runs are maintained within the system and are generally limited to the user
- **Content of files accessed/reviewed**	X	A	Audit logs of files accessed are stored and reviewed by administrators
- **Contents of files**	X	A	Contents of all files are available to administrators
Other (please list the type of info and describe as completely as possible):	X	A and B	PIV card or other identification document

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):					

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

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**	**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 Security and Facilities Management Section (SFMS) may receive requests from other internal organizations to provide access logs to identify user entry and exit of sensitive areas within the facility. These requests are rare, and the information provided is limited based on source of request and information requested.
DOJ Components			✓	ATR Security and Facilities Management Section (SFMS) provides system logs to DOJ's centralized access control service managed by SEPS. JMD SEPS owns the PACS logs for MJB and LSB, and has accounts to log in and obtain the logs.
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

ATR PACS is an internal physical security management system used to manage and control access to and from ATR facilities. ATR does not release data or documents to the public regarding physical security controls, logs, or data. 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.

To alert employees of and visitors to ATR facilities of the possibility that they will be captured in video images, ATR posts signage alerting of continuous video surveillance within secured government facilities.

Additionally, two SORNs provide generalized notice to the public:

(1) DOJ-011, "Access Control System (ACS)," 69 Fed. Reg. 70279 (12-03-2004), available at https://www.govinfo.gov/content/pkg/FR-2004-12-03/pdf/04-26590.pdf; and

(2) GSA/GOVT-7, "HSPD-12 USAccess," 80 Fed. Reg. 64416 (10-23-2015), available at https://www.federalregister.gov/documents/2015/10/23/2015-26940/privacy-act-of-1974-notice-of-an-updated-system-of-records.

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.

ATR PACS is an automated system that uses sensors and automated devices to collect and manage physical security information from cameras and door scanners. Appropriate signage is used throughout ATR facilities notifying individuals of the use of video and physical surveillance to protect the facility. Additionally, information collection is required to facilitate entrance into an ATR facility. Therefore, it is presumed that entry into secure facilities signifies consent to participate in this collection. An individual who objects to these facility security measures will not be allowed to access the facility.

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 follows Department procedures regarding requests for access to, or amendment of, records pertaining to an individual and maintained within a system of records, in accordance with the Privacy Act. See https://www.justice.gov/opcl/doj-privacy-act-requests. Privacy Act requests for access to records are processed under both the Privacy Act and the Freedom of

Information Act (FOIA), 5 U.S.C. § 552. All such requests are submitted to ATR's FOIA/Privacy Act Unit (https://www.justice.gov/atr/antitrust-foia) for processing and response.

Section 6: Maintenance of Privacy and Security Controls

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

✓	**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):** 4/2/2020 **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 currently no open POAMs within the profile.
	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:** ATR PACS 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's primary infrastructure environment, ATR General Support System (GSS), where it is subject to full system monitoring and audit in accordance with ATR and Department guidelines. All system documentation supporting these activities are maintained within the Department's system of record, Cyber Security Assessment and Management (CSAM) tool.
✓	**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 PACS audits at multiple layers, including the network and application processing levels. All logs are generally reviewed on a weekly basis by onsite administrators and then gathered and centrally managed using the Department's audit analysis solution, Splunk Enterprise application (SPLUNK). All logs are forwarded to the DOJ JSOC for automated analysis and review, as well as the DOJ SEPS Security Team, in compliance with Department physical security guidelines.

✓	**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 PACS are required to sign the DOJ Non-Disclosure Agreement and 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.
✓	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All PACS users are subject to organizational and Department annual computer security awareness and privacy specific training that includes sign off and acknowledgment of the DOJ General and Privileged Rules of Behavior. In addition, personnel who have specific administrative roles within the application require and have received specialized role-based training, both prior to starting their position and as needed.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

All ATR facilities have physical access controls in place, such as guarded buildings with one main entrance to process flow of guests into the facility, protocols in place to check for government issued IDs, parking in a secured area available for employees and visitors who arrange parking in advance of a visit. All ATR PACS operators and administrators are security specialists and are required to use multi-factor authentication to access the ATR network prior to accessing the ATR PACS portal. They then must use a unique username and password to access their ATR PACS accounts. All data is encrypted at rest and during transmission outside of ATR's secure boundary. Only ATR operations and physical security personnel are authorized to access ATR PACS. All ATR PACS users are required to undergo training and sign formal Rules of Behavior prior to being granted access to ATR PACS devices or data. Additionally, ATR PACS will maintain a limited system log that captures users' activities during each user sessions. These sessions can be reviewed by the primary admin account or system owner.

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.)

PACS is an internal office tool, and information contained within it is generally retained in compliance with DOJ guidelines of 90 days online and one year offline and archived for up to 7 years in compliance with Department data archiving standards.

PACS contains only physical security access information and facility security surveillance data, such as video camera imagery, badging information, and PIV credentials. This information is retained in accordance with DOJ policy and shared with the Department SEPS security team for appropriate analysis and archiving.

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:

DOJ-011, "Access Control System (ACS)," 69 Fed. Reg. 70279 (12-03-2004), available at https://www.govinfo.gov/content/pkg/FR-2004-12-03/pdf/04-26590.pdf.

GSA/GOVT-7, "HSPD-12 USAccess," 80 Fed. Reg. 64416 (10-23-2015), available at https://www.federalregister.gov/documents/2015/10/23/2015-26940/privacy-act-of-1974-notice-of-an-updated-system-of-records.

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 overcollection of information, information in ATR PACS is limited to individuals who enter an ATR facility, and the information about them that is relevant and necessary to perform building security. While video and photo surveillance devices may capture images of members of the public who incidentally pass an ATR facility, the privacy risks associated with those images are minimal as the individuals are not identified, categorized, tracked, or managed and the

images are not associated with any additional PII.

Additionally, appropriate signage is posted in all publicly accessed locations, alerting to the use of video surveillance in the area, and the Department has published SORNs to cover this collection.

To mitigate the risk of unauthorized access to or disclosure of the information in PACS, information is shared with only approved authorized users either through direct log on to ATR PACS or through other secure means, such as internal email or secure file transfer. Only information that is necessary for accomplishment of each individual's duties is shared. In addition, individuals are required to take Computer Security and Awareness Training (CSAT) annually to provide proper user training.

Additionally, PACS users are divided into operators and administrators. Only the administrators have additional access into the system to print and review log files and share relevant information when needed. Only authorized ATR PACS operators and administrators can access ATR PACS. Access is even further limited by Access Control Lists that are implemented and maintained by the data owners and is limited to the Technology Services Section Operations team and the Security and Facilities Management Unit personnel. All system information and logs are kept online for up to 90 days, offline for one year and archived for up to 7 years in compliance with Department data archiving standards.