Antitrust Division

Privacy Impact Assessment
for the
Antitrust Physical Access Control System - Cloud
(ATR PACS-C)

Issued by:
Sarah Oldfield
Senior Component Official for Privacy

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

Date approved: February 29, 2024

(May 2022 DOJ PIA Template)

Points of Contact and Signatures

COMPONENT PRIVACY POINT OF CONTACT (POC) Name: Sarah Oldfield Office: Office of the Chief Legal Advisor Phone: 202-305-8915 Bldg./Room Number: RFK/3304 Email: sarah.oldfield@usdoj.gov	**PIA AUTHOR** (if different from POC) Name: Sherod Emerson Office: Information System Security Officer Phone: 240-565-5807 Bldg./Room Number: LSB Email: sherod.emerson2@usdoj.gov
SECURITY REVIEW OFFICIAL (Component CIO/OBD Executive Officer/OCIO Staff Director/JMD Staff Director) Name: Kobie Crawl Office: Director of Technology and CIO, Technology Directorate Phone: 202-227-1017 Bldg./Room Number: LSB/3622 Email: kobie.crawl@usdoj.gov Signature: KOBIE CRAWL Digitally signed by KOBIE CRAWL Date: 2024.04.08 09:13:31 -04'00' Date signed:	**SENIOR COMPONENT OFFICIAL FOR PRIVACY** (if designated; otherwise POC) Name: Sarah Oldfield Office: Office of the Chief Legal Advisor Phone: 202-305-8915 Bldg./Room Number: RFK/3304 Email: sarah.oldfield@usdoj.gov Signature: SARAH OLDFIELD Digitally signed by SARAH OLDFIELD Date: 2024.04.08 12:12:37 -04'00' Date signed:

DOJ PIA APPROVING OFFICIAL
Katherine M. Harman-Stokes
Director (Acting)
Office of Privacy and Civil Liberties
U.S. Department of Justice
(202) 616-5485

Signature: KATHERINE HARMAN-STOKES Digitally signed by KATHERINE HARMAN-STOKES Date: 2024.04.01 13:11:11 -04'00'

Date signed:

THIS PAGE IS FOR INTERNAL ROUTING PURPOSES AND DOCUMENTATION OF APPROVALS. UPON FINAL APPROVAL, COMPONENTS SHOULD REMOVE THIS PAGE PRIOR TO PUBLICATION OF THE PIA.

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

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 (ATR) Physical Access Control System – Cloud (ATR PACS-C) is an Infrastructure as a Service electronic security system used to control employee and visitor access to ATR facilities housed in the ATR Cloud Computing Environment (CCE). PACS-C is an IaaS solution. The system monitors, logs, records, and alerts on the interior and exterior portions of the facility. ATR PACS-C will replace the existing physical access control (Physical Access Control System, an on-premises solution) and monitoring system.

ATR PACS-C processes and stores DOJ personnel data associated with PIV cards. This information includes personnel name, organization, office location, facility access rights and privileges, and entry and exit of facilities. ATR PACS-C will also process, and store information associated with building entrances and monitoring. For instance, ATR personnel, authorized individuals, and individuals who enter or approach ATR facilities are recorded on ATR video cameras, and their images are displayed on security monitors. License plate numbers of personnel and visitors authorized to park in ATR facilities are also video recorded and displayed on security monitors. ATR PACS-C does not use facial recognition technology.

ATR PACS-C contains information in identifiable form relating to DOJ personnel and members of the public. As such, ATR is publishing this PIA to fulfill the requirements of 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 PACS-C is an electronic security system used to control, manage, and monitor employee and visitor access to ATR facilities. The system allows control of personnel and visitor physical access to DOJ facilities and provides authorized personnel administrative access to manage system logs and physical access to gates, doors, and barricades. Additionally, the system monitors user access via video feeds, logs, records, and alerts on the interior and

exterior portions of the facility.
All visitors must access ATR facilities through the main entryway. Generally, only authorized employees with their vehicles can enter through the garage of the building. Some locations may allow visitor parking if pre-arranged. Foreign National visitors enter and are processed in the main entry only with badges that indicate they must be escorted at all times.

As previously provided, ATR PACS-C has replaced the existing physical access control and monitoring system to provide greater redundancy and resilience in its implementation of centralized physical access controls, alerts, alarms, and monitoring capabilities. ATR PACS-C has been deployed using a client-server architecture that will interconnect all devices and offices using DOJ's trusted long-haul communications backbone, the Justice Unified Telecommunications Network (JUTNet) Wide Area Network (WAN), as a gateway, the ATR Cloud Computing Environment as the processor, and provide feeds to DOJ's centralized access control service managed by SEPS.

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	28 C.F.R. §§ 0.40, General functions, and 0.41, Special functions
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, D	Names of employees and personnel. Additionally, visitor names will be captured in the system
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity, or citizenship	X	A. B, C, D	Race or ethnicity may be captured in camera images. No audio.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	X	A, B, C, D	Vehicle information may be captured in camera images in garages or parking lots
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information	X	A, B, C, D	Medical or health information may be captured in camera images
Financial account information			
Applicant information			
Education records			
Military status or other information	X		Military status may be captured in camera images
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			

(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
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, D	Photographic and imagery data is collected from cameras deployed on the interior and exterior of ATR facilities
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	A, B, C, D	Scars, marks and tattoos may be captured in camera images
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	ATR PACS-C is operated and administered by DOJ government and contractor personnel

(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 ID**	X	A	All administrators are provided unique user IDs
- **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 data 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
- **Contents of files**	X	A	Audit logs of files accessed are stored and reviewed by administrators; Contents of all files are available to administrators
Other (please list the type of info and describe as completely as possible):	X	A, 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	✓	Other federal entities	
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 SFMS provides system logs to DOJ's centralized access control service managed by SEPS. JMD SEPS owns the ATR PACS-C 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				

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.**
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-C 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/0426590.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-actof-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-C 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): **If an ATO has not been completed, but is underway, provide status or expected completion date: Package is underway. Planned completion: 31 Mar 2024** **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 POA&Ms associated with Privacy Controls.
	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:
✓	**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 PACS-C is categorized as a moderate system based on a review of the aggregate impact levels for confidentiality, integrity, and availability.
✓	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** ATR PACS-C 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 CCE, 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, Joint Cybersecurity Authorization and Management (JCAM) 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-C 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-C are required to sign the DOJ Non-Disclosure Agreement and the DOJ General and/or Privileged Rules of Behavior, as determined by their role.
✓	**Each Component is required to implement foundational privacy-related training for all Component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All ATR PACS-C 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-C operators and administrators are security specialists or technicians and are required to use multi-factor authentication to access the ATR network prior to accessing the ATR PACS-C portal. They then must use a unique username and password to access their ATR PACS-C accounts, with the exception of one contracted support technician who utilizes a generic administrative service account to provide assistance. 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-C. All ATR PACS-C users are required to undergo training and sign formal Rules of Behavior prior to being granted access to ATR PACS-C devices or data. Additionally, ATR PACS-C 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-C 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.

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-1974notice-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-C 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-C, information is shared with only approved authorized users either through direct log on to ATR PACS-C 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.

Additionally, PACS-C 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-C operators and administrators can access ATR PACS-C. 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.