United States Department of Justice (DOJ)

Office of Privacy and Civil Liberties (OPCL)

Privacy Impact Assessment
for
USACCure

Issued by:
Kevin S. Krebs – Senior Component Official for Privacy

Approved by: Christina Baptista, Senior Counsel
Office of Privacy and Civil Liberties Officer
U.S. Department of Justice

Date approved: October 30, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The USACCure system is EOUSA's new physical access system that will replace the current Hirsch Velocity System. The USACCure provides physical access control for personnel entering or exiting DOJ facilities via badge card readers. The system also performs network video recording via IP cameras for intrusion detection purposes. A PIA was performed for USACCure because it is an information technology that involves the collection, maintenance, and dissemination of information in identifiable form, including names, contact information, photographs, and video.

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.

USACCure is EOUSA's new Physical Access Control System (PACS) that will replace the current Hirsch Velocity System. USACCure provides physical access control and video surveillance for personnel entering and exiting DOJ facilities via badge card readers and IP cameras. USACCure utilizes iSTAR access control panels. CCure 9000 is a security management system that provides a standard approach to physical access authorization throughout DOJ facilities.

USACCure also utilizes the Innometriks service as the FICAM solution. Innometriks provides High Assurance Smartcard, Biometric, and PIN authentication for the CCure PACS. The solution consists of the Enrollment Plug-in and the Panel Service in CCure along with compatible readers and iSTAR panels with High Assurance enabled.

Additionally, the CCure application will be integrated with the Victor Video Management application which is a globally scalable solution optimized for command and control that seamlessly synchronizes video surveillance with access control, intrusion detection, and other systems into one powerful, intuitive interface.

USACCure also consists of Mobile Credential Units and Light Activation Kits. The Mobile Credentialing Unit (MCU) is the credential kit for PIV cards which is leased from GSA. EEUT has implemented their image on the GSA-leased workstations. These workstations are currently on the EOUSA network and are dedicated for the use of the MCU kit. The Light Activation Kit is a software installed on a standard EOUSA workstation. The Light Activation Kit is used to allow activation of USAaccess credentials and perform post issuance activities, such as certificate updates and PIN resets.

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	5 USC § 301 40 U.S.C. § 11101 44 USC § 3301 44 USC § 3502 28 USC Ch. 35 Federal Information Security Modernization Act of 2014, 44 USC § 101 note
Executive Order	Homeland Security Presidential Directive 12
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019)

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,	First and Last Name
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity, or citizenship			
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			

(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
Vehicle identifiers			
Personal mailing address			
Personal e-mail address	X	A, B	
Personal phone number	X	A, B	
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
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	X	A, B	IP address, computer names, MAC address
Web uniform resource locator(s)	X	A, B	Enabled only for administrative purposes
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	X	A	Email address
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B	Photos for DOJ employees/contractors

(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
- **Video containing biometric data**	X	A, B, C D	Videos for all individuals
- **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 passwords/codes**	X	A	
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):			

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		Online	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
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	X	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	X	X	X	Auditing and Investigation purposes
DOJ Components	X	X	X	Auditing and Investigation purposes
Federal entities	X			Auditing and Investigation purposes
State, local, tribal gov't entities				
Public	X			FOIA requests
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Case investigation 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.

Not Applicable

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021), https://www.justice.gov/opcl/page/file/1419896/download.

DOJ-011, Access Control System (ACS), last published in full at 69 Fed. Reg. 70279 (Dec. 3, 2004), https://www.govinfo.gov/content/pkg/FR-2004-12-03/pdf/04-26590.pdf

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.

There are no opportunities given to individuals to decline providing the requested information. Declining providing the requested information will result in users being prohibited from accessing 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.

Individuals may request access to information in the system pertaining to them by visiting the following website for component-specific instruction: https://www.justice.gov/usao/resources/making-foia-request

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):** ATO granted on 2/8/2023 and expires 2/8/2026. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs)**

	for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation: There are no POA&Ms in relation to 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: Not Applicable
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:** As mentioned in the System Security Plan, the USACCure has been categorized as a moderate system with confidentiality, integrity, and availability levels marked as moderate as well.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Moderate baseline controls are implemented. TLS 1.2 is utilized for transmission of data and AES 256 is utilized for encryption at rest. Audit logs are forwarded to the SIEM (Security Information and Event Management) solution.
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:** USACCure generates audit records containing information that establishes what type of event occurred, when the event occurred (date/time), where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. The USACCure Information System Security Officer (ISSO) is responsible for reviewing all audit logs on a weekly basis from the SIEM solution. The DOJ Core Controls are assessed at least annually. A full assessment of all security controls is performed at least every three years.
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:** Security Awareness Training and Role-Based Training are required for all EOUSA personnel and are offered by LearnDOJ.

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?

Access controls are implemented to ensure only authorized users have access to the information collected, in addition to only being granted the privileges necessary to accomplish their job duties. Additionally, there are safeguards implemented to ensure that unauthorized access to the system is not granted and the risk of unauthorized disclosure of the information within the system is minimized.

All login actions are audited to ensure that no unauthorized users have been granted access to the system and all audit logs are reviewed on a weekly basis by the ISSO. An open session within the information system will also be subject to session termination in cases of inactivity.

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.)

The data in the USACCure system is maintained for as long as needed by the authorized DOJ users and are subject to the respective retention periods that govern them, e.g., NARA General Records Schedules, agency SF-115s, and any applicable SORNs published under the Privacy Act of 1974, 5 U.S.C. §552a (see https://www.justice.gov/opcl/doj-systems-records). Procedures have been developed to ensure that electronic copies are not in practice retained beyond the retention period established for the original records and will be disposed of in accordance with DOJ Network Account Records Management USAP No. 3-13.300.004.

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.

7.1 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-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021), https://www.justice.gov/opcl/page/file/1419896/download.

DOJ-011, Access Control System (ACS), last published in full at 69 Fed. Reg. 70279 (Dec. 3, 2004), https://www.govinfo.gov/content/pkg/FR-2004-12-03/pdf/04-26590.pdf

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?

The USACCure provides physical access control of personnel entering / exiting DOJ facilities via badge card readers. The system also performs network video recording via IP cameras for intrusion detection purposes.

The disclosure or sharing of information increases risks to privacy. However, there are measures taken to reduce the risk of unauthorized disclosure and potential data breach. All EOUSA component systems are subject to regular periodic assessment and authorization processes that ensure that security controls are in place to protect the confidentiality, integrity, and availability of all information and the systems that house that information.

The principle of least privilege will be enforced to ensure those who have access are only granted the minimum access required based on job duties. All EOUSA component staff require mandatory security awareness and role-based training on an annual basis.

Additionally, security controls will be tested during the assessment process and prior to system authorization. Other security control families that are tested and implemented as safeguards include: Auditing, Contingency Planning, Incident Response, Media Protection, Physical Protection, Risk Assessment, and System and Information Integrity.