United States Department of Justice (DOJ)
Office of Privacy and Civil Liberties (OPCL)

Privacy Impact Assessment
for the
USA Visitor Management System (USAVMS)

Issued by:
Kevin Krebs, Senior Component Official for Privacy

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

Date approved: July 19, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The USA Visitor Management System (USAVMS) is a physical access control system that provides a single unified interface that will handle the physical security access requests to Executive Office for United States Attorneys (EOUSA) and United States Attorneys (USA) facilities across the entire organization. USAVMS runs on HID SAFE which is a Commercial Off-The-Shelf (COTS) software.

USAVMS automates end-user-initiated requisition and approval workflows, allowing physical security practitioners to respond efficiently to multiple physical security requests. The system monitors, logs, and records requests from DOJ personnel, contractors and the public for access to EOUSA/USA facilities.

USAVMS will collect identification and contact information on DOJ employees, contractors, other federal government visitors and members of the public visiting DOJ facilities; biographical information on visitors; and date, time, and purpose of visitors' appointments. USAVMS will process and store DOJ personnel data associated with PIV cards. This information includes personnel name, organization, office location, facility access rights and privileges, and the entry and exit of facilities. The system will also store information related to employee and contractor requests for a new badge or physical key.

USAVMS contains information in identifiable form relating to DOJ personnel, other government personnel visitors, and members of the public. As such, EOUSA 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.

USAVMS is an electronic security system that runs on the HID SAFE software which increases efficiencies by enabling authorized personnel to have the software installed on their workstations. Users can make multiple physical security requests on their own through the desktop application or by accessing the web client. These requests range from requesting physical access to a DOJ facility to changing existing access for an individual. USAVMS also enables employees to pre-register visitors, which offloads the burden of the front-desk personnel. USAVMS allows a host to check visitors in and out of the facility. Visitors may check-in to a facility and provide their ID to be scanned, or they can have their photos taken prior to entering the facility These visitor records are stored within the system.

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 U.S.C. § 301 • 28 USC Ch. 35 • Federal Information Security Modernization Act of 2014, 44 USC § 101 note.

Executive Order	• Executive Order 12977, "Interagency Security Committee"; • Homeland Security Presidential Directive-7 (HSPD-7), "Critical Infrastructure Identification, Prioritization and Protection"; • Executive Order 13286, "Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security"; • Homeland Security Presidential Directive 12, "Security Awareness and Reporting of Foreign Contacts"; • Homeland Security Presidential Directive-7 (HSPD-7), "Critical Infrastructure Identification, Prioritization and Protection" • OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019).
Federal regulation	• 48 C.F.R. §§ 24.104, 52.224-1 to -2 (2019).
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	First and Last 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
Date of birth or age	X	A, B	Date of Birth. Users may decline to provide this information, however, if the information is not provided, access to the facility will not be granted.
Place of birth			
Sex	X	A, B	Users may decline to provide this information, however, if the information is not provided, access to the facility will not be granted.
Race, ethnicity, or citizenship	X	A, B	Ethnicity. Users may decline to provide this information, however, if the information is not provided, access to the facility will not be granted.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license	X	C, D	Users may decline to provide this information, however, if the information is not provided, access to the facility will not be granted.
Alien registration number	X	C, D	Residency cards, work authorization cards. Users may decline to provide this information, however, if the information is not provided, access to the facility will not be granted.
Passport number	X	C, D	Users may decline to provide this information, however, if the information is not provided, access to the facility will not be granted.
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C, D	House / Apt Number, Street Name, City, State, Zip Code
Personal e-mail address	X	A, B, C, D	Personal email address
Personal phone number	X	A, B, C, D	Personal phone number
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information	X	A, B, C, D	First and Last Name; personal email address, personal phone number of DOJ employees and contractors, other government personnel and visitors from the public.
Education records			

(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
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			
Web uniform resource locator(s)	X	A, B	Web URL is only accessible by internal DOJ users
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	C, D	Scans of drivers' license, passport and/or other forms of ID. Visitors may also have their photograph taken to enter a facility.
- Video with biometric data			
- Fingerprints			
- Palm prints			
- Iris image			
- Dental profile			

(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
- **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, B	System event logs: username.
- **User passwords/codes**			
- **IP address**	X	A, B	System event logs: IP address
- **Date/time of access**	X	A, B	System event logs: date/time
- **Queries run**	X	A, B	System event logs: actions, username, date/time, IP address, system data.
- **Contents of files**	X	A, B	System event logs: actions, username, date/time, IP address, system data.
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	X	Email	X		
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	X

Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

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

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**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	
DOJ Components	X			Requests from sister components for investigation purposes to address physical security or cyber security related incidents.
Federal entities	X			Requests from federal entities for investigation purposes to address physical security or cyber security related incidents.
State, local, tribal gov't entities	X			Requests from local and/or state entities for investigation purposes to address physical security or cyber security related incidents.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Requests from counsel and/or court orders for litigation purposes, such as to provide visitor record evidence of a district office supporting a defense attorney or prosecutor case.
Private sector	X			Requests from counsel and/or court orders for litigation purposes, such as to provide visitor record evidence of a district office supporting a defense attorney or prosecutor case.
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.

The records contained within the system include Personal Identifiable Information (PII) such as names and photos of individuals. This system is only accessible internally and there is no intention of making the information public.

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.

Generalized notice is given in the below published SORNs:

DOJ-002 DOJ Computer Systems Activity & Access Records, last published in full at 64 FR 73585 (12-30-1999), https://www.govinfo.gov/content/pkg/FR-1999-12-30/pdf/99-33838.pdf.

DOJ-011 Access Control System (ACS), last published in full at 69 FR 70279 (12-03-2004), 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.

USA staff are not provided the opportunity to opt out of participating in the collection, use, or dissemination of their information in the system. USA staff who do not utilize the system may be unable to perform their job functions or access services requested through the system. Although members of the public may choose to decline providing information, doing so may result in denial of entry to the facility until the requested information is provided.

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.

The authoritative sources for visitor information are the visitors themselves. After the information is provided by the visitors, the record is not available for modifications or amendment as it represents a static point in time. If any corrections are needed, the visitor can request a correction or modification from their sponsor.

Individuals may also make a FOIA request to access 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.

Additional information regarding access to information may be found in the SORNs listed in

section 5.1.

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 December 2, 2022, and expires on December 9, 2025. **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:** POAM 40547 is open to track approval of the IPA and PIA
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Based on the identified information types, the system has been categorized as a Moderate level system.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Moderate baseline controls are implemented which include Access Control, Audit and Accountability, Encryption, and System and Information Integrity. USAVMS 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. USAVMS is configured to forward audit records to the USA Advanced Analytics Platform (USAP-AAP) (Splunk). The USAVMS Information System Security Officer (ISSO) is responsible for reviewing all audit logs on a weekly basis.
	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted: USAVMS 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

X	with the event. USAVMS is configured to forwarded audit records to USAP-AAP (Splunk). The USAVMS Information System Security Officer (ISSO) is responsible for reviewing all audit logs on a weekly basis.
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:** EOUSA provides security-awareness and role-based training specific to the system for authorized users within the organization.

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. Encryption is implemented in transit and at rest to protect system data.

Separately, physical access to facilities is monitored by security guards and surveillance cameras with man traps in place to control ingress and egress of individuals.

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 USAVMS 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 are in place to ensure that electronic copies are not 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.

7.2 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-002 DOJ Computer Systems Activity & Access Records, last published in full at 86 FR 37188 (July 14, 2021), https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.

DOJ-011 Access Control System (ACS), last published in full at 69 FR 70279 (12-03-2004), 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 disclosure or sharing of information inherently 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 consistent 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.

All login actions are and will be audited to ensure no unauthorized users have been granted access to the system. 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 to ensure unauthorized access to the system is not granted and to minimize the risk of unauthorized disclosure.

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: Access Control, Audit and Accountability, Contingency Planning, Incident Response, Media Protection, Physical and Environmental Protection, Risk Assessment, System and Communications Protection, Configuration Management, and System and Information Integrity.