United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for
DOJ Login

Issued by:
Morton J. Posner
JMD Senior Component Official for Privacy

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

Date approved: [April 9, 2024]

(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 Federal Information Security Modernization Act of 2014 requires that Federal agencies, including the United States Department of Justice (DOJ or "the Department"), comply with certain information security policies and procedures. Such policies and procedures require agencies to properly identify, credential, monitor, and manage individuals who access Federal resources, including information, information systems, facilities, and secured areas. DOJ's compliance with the Federal Identity, Credential, and Access Management (ICAM) policy is essential to meeting DOJ's information security and privacy risk management responsibilities.

The purpose of the DOJ Login is to provide a web-based, multifactor authentication for DOJ applications to DOJ workforce, Federal agencies, and business partners. DOJ Login will include members of the public who have business with the Department and/or need to access a Department information system. The Department is completing this Privacy Impact Assessment because DOJ Login will require Federal agency users, business partners, and members of the public with business with DOJ or a need to access DOJ systems, to register for credentials through DOJ Login, submit key pieces of information for authentication purposes (i.e., name, email address, and phone number), and be approved for access by the corresponding DOJ application owner for which they are requesting access.

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.

The Identity, Credential, and Access Management (ICAM) program provides a comprehensive approach for dealing with digital identities (and associated identity attributes), credentials, and access control helping to address the growing data management, interoperability, and cybersecurity challenges facing agencies today. The mission of the ICAM program is to align core security services and IT investments to enable secure access to systems and applications through verified identities and trusted credentials.

Three strategic goals help set the target for the program:

1. Improve security of DOJ resources
2. Securely share information with external communities
3. Automate on-boarding and off-boarding

To accomplish these goals, the DOJ team that implements the ICAM program creates and maintains policies, processes, and procedures that govern the strategic planning, implementation, and evaluation of the overall program. Governance is at the core—unifying identity, access and credential management to support application, cloud, and mobile security.

Within the ICAM program, DOJ Login supports both improving the security of DOJ resources and facilitating secure information sharing with external communities. At its core, DOJ Login provides secure access to DOJ applications and information systems via Authentication Assurance Level (AAL) 3 access for internal DOJ users, and AAL2 access for external users. DOJ ICAM policy requires AAL2 and higher authentication for users accessing DOJ applications and information systems. DOJ Login enables higher-authentication assurance access even for applications which natively do not support access at AAL2 or higher. AAL 2 and AAL3 are defined by the National Institute of Standards and Technology (NIST) as:

> **AAL2:** AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above. *Example: sign in via username and password (Factor 1) plus a mobile application one-time passcode (Factor 2).*
>
> **AAL3: A**AL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication SHALL use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device MAY fulfill both these requirements. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required. *Example: User signs in with a government issued SmardCard, such as a Personal Identity Verification (PIV card).*

DOJ Login uses Okta Identity Cloud[1] and provides a mechanism to use a wide variety of multifactor authentication methods for all users. For users who have PIV cards (in most cases, DOJ workforce or other Federal agency users) enabling AAL3, Okta uses attribute-based policy enforcement to require users to use their PIV card to access a DOJ application, even if the connected application is not inherently PIV-enabled. For users who do not have a PIV card (e.g., they are in the process of obtaining a PIV card or are not Federal employees/contractors or do not qualify for a PIV card), DOJ Login will use a username/password and a second authentication method (i.e., Okta Verify, Google Authenticator, or Email-Link Verification) to

[1] The Okta Identity Cloud is an independent and neutral platform that is designed to securely connect the right people to the right technologies at the right time. It's an enterprise-grade identity management service built for the cloud, but compatible with many on-premises applications. With Okta, an organization can manage any employee's access to any application or device. As stated in Okta product materials, Okta runs in the cloud, on a secure, reliable, extensively audited platform, which integrates deeply with on-premises applications, directories, and identity management systems. Additional information is available at: https://www.okta.com/products/

support AAL2.[2] Once authenticated, users will have access through the web-based portal application and the respective resources based on access granted by application owners.

Okta Identity Cloud will extend these online offerings to have the ability for users to sign-in, access a portal for seamless access to approved applications, and recover credentials via self-service portal (or with assistance from customer support). The Okta Identity Cloud is embedded as the identity layer of DOJ Component portals to protect customer accounts while providing the optimal user experience across applications.

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	Federal Information Security Modernization Act of 2014, Pub. L. 113- 283, 128 Stat 3073; 40 U.S.C. 1441 note, requiring Federal Agencies to plan for the security and privacy of their computer systems
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	Office of Management and Budget M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019). https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

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

[2] An authentication process that "requires more than one distinct authentication factor for successful authentication" is commonly referred to as multi-factor authentication (MFA)—"The three authentication factors are something you know, something you have, and something you are." *See* NIST SP 800-63-3, *Digital Identity Guidelines* (June 2017).

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	Required for managing users of the DOJ Login using Okta Identity Service to allow deployment of pre-integrated applications to users. DOJ Login accounts are created leveraging the user's name. Business partners (both Federal, State, Local, Tribal and Territorial (SLTT), and private) will access DOJ applications utilizing DOJ Login. In some cases, citizens, legal residents, and members of the public might need to access their information within certain DOJ applications.
Date of birth or age			
Place of birth			
Gender			
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			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address	X	C, D	If a business email address is not provided, then personal email addresses are used for managing users who are citizens, legal residents, and members of the public.

(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 phone number	X	C, D	If the user agrees to use their phone for multifactor authentication, a phone number would be used to send a text message to the user's stored phone number to authenticate the user.
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			
Web uniform resource locator(s)			
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			

(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
Biometric data:			
- **Photographs or photographic identifiers**			
- **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, B, C, D	DOJ Login keeps audit logs of all functions, but the logs are read-only. This includes userID, authentication factors used (including use of passwords, PIV, and MFA), IP address, and date/times of activity.
- **User passwords/codes**	X	A, B, C, D	DOJ Login does not audit or make visible user passwords. However, DOJ Login keeps audit logs of UserID and authentication factors used (including use of passwords, PIV, and MFA), IP address, and date/times of login.
- **IP address**	X	A, B, C, D	DOJ Login keeps audit logs of all functions, but the logs are read-only. This includes userID, authentication factors used (including use of passwords, PIV, and MFA), IP address, and date/times of activity.
- **Date/time of access**	X	A, B, C, D	DOJ Login keeps audit logs of all functions, but the logs are read-only. This includes userID, authentication factors used (including use of passwords, PIV, and MFA), IP address, and date/times of activity.
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			

(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
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		Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify): In certain circumstances, individuals may utilize email or mobile devices for Time-based One-Time Password (TOTP) PIN verification during the MFA process.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	X
State, local, tribal	X	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	X
Commercial data brokers					
Other (specify): In certain circumstances, individuals may utilize approved authenticator applications offered by private sector entities during the MFA process.					

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			DOJ Login activity is monitored by the Justice Security Operations Center (JSOC) for Indicators of Compromise (IOC) and Incident Response (IR). JSOC incident response (IR) personnel have permission to view and monitor user logs in DOJ Login for IOCs. Additional access may be granted on a case-by-case basis to support IR as required.
DOJ Components	X			DOJ Login is a part of a federation of Identity, Credential, and Access Management systems, thus basic user information for authentication purposes will be shared between Component systems to facilitate user-specific application access; only administrators would be able to access that information. Information is shared based on application needs for categories of users.
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.

DOJ Login information will not be released to the public for "Open Data" or for research or statistical analysis purposes.

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.

The Department has notified individuals of the system's collection, use, and sharing of records by way of applicable System of Records Notices: JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021), and, DOJ-020, DOJ Identity, Credential, and Access Service Records System, 84 Fed. Reg 60110 (Nov, 7, 2019).

In addition, DOJ Login users are presented with a privacy notice as follows:

You are accessing U.S. Government information technology and/or information systems which includes: (1) this information technology, (2) this information system, (3) all information technology devices connected to this network, and (4) all devices and storage media attached to this information system or to information technology on this network.

This information technology and information system is provided for U.S. Government-authorized use only. You have no reasonable expectation of privacy when using this information technology and/or information system and the government may monitor, intercept, search and/or seize data transiting through or stored within. Unauthorized or improper use may result in disciplinary action as well as civil and/or criminal penalties.

A link to DOJ's full privacy policy is available on the DOJ Login user dashboard: https://www.justice.gov/doj/privacy-policy.

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.

Individuals that wish to access DOJ information systems that leverage DOJ Login for its

authentication processes must participate, as DOJ Login provides necessary security measures required for DOJ information systems to complete the operation of the system.

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 have been notified that the account, audit log, and user records maintained in DOJ Login can be accessed or amended in accordance with DOJ Privacy Act system of records notices (SORNs): JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021) and DOJ-020, DOJ Identity, Credential, and Access Service Records System 84 Fed. Reg 60110 (Nov, 7, 2019).

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):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** ATO issued 04/12/2023 **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:**
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** FedRAMP requires vulnerability and configuration scans monthly. Okta completes required scans and makes available to customers. An elected personnel will review the vulnerability and configuration scans to ensure vulnerabilities are being patched in a timely manner.
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: Logs are collected daily.
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:** All DOJ users must complete computer security awareness training annually, as well as read and agree to comply with DOJ information technology Rules of Behavior both prior to accessing the DOJ network and annually thereafter. System administrators, including DOJ Login Administrators, must complete additional professional training, which includes security training.

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?

A full security control assessment has been completed for DOJ Login, to include logical access, identification and authentication, vulnerability management, auditing, etc. DOJ Login makes use of separate Privileged and Non-Privileged user accounts and leverages additional role-based access control technologies and administrator session recording. All system and application log data will be sent to DOJ's centralized audit log management system for triage and review. The CSS Information Security System Officers (ISSOs) are charged with reviewing logins and performing auditing functions to ensure role-based access controls satisfying the above measures.

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.)

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule 3.2, for records created and maintained by Federal agencies related to protecting the security of information technology systems and data, and responding to computer security incidents. Log data will be maintained in Logging as a Service as the DOJ's repository for 365 days.

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:

JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021); and

DOJ-020, DOJ Identity, Credential, and Access Service Records System, 84 Fed. Reg 60110 (Nov, 7, 2019).

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.***

DOJ Login enables web-based, multifactor authentication to DOJ applications for DOJ workforce, Federal agencies, business partners, and members of the public. DOJ Login collects only the PII required for purposes to authenticate a user at AAL2, which includes names, personal e-mails addresses, personal phone numbers, and system admin/audit data (e.g., user IDs, user passwords, IP addresses, date/time of action). DOJ login information is retained in accordance with National Archives and Records Administration (NARA) schedules. Data minimization strategies including data retention is determined on the tool, service, or application level. DOJ Login does not collect certain data types for its users (such as Social Security Numbers and Tax Identification Numbers) to minimize the collection of PII.

Sources come directly from users, DOJ Active Directories (AD) and/or from IamDOJ[3], which auto provisions attributes for the DOJ workforce. DOJ Login implements encryption, account management, access controls, and auditing to mitigate and protect personally identifiable information. DOJ Login makes use of separate Privileged and Non-Privileged user accounts and access is granted on least privilege and need-to-know requirements.

Information is shared through direct login access within the Component or other, connected DOJ Components. DOJ Login uses encryption and logging controls for mitigation purposes. DOJ Login makes use of Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2, to protect data in transit between the browser and the user's workstation. The DOJ Login Information System Security Officer performs continuous monitoring of the security controls within the system to ensure security protections are operating as intended.

By Department Order, all DOJ users with access to Department networks, including DOJ Login, must receive an annual Cyber Security Assessment Training (CSAT). The course explains personally identifiable information and key safeguards, identifies potential risks and vulnerabilities associated with using DOJ-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also annually sign a DOJ Rules of Behavior agreement confirming that they have completed this course and that they agree to abide the stated requirements, including Privacy Act compliance. Failure to successfully complete this training can result in termination of the employee or contractor's access to DOJ computers. Participation in the training course is tracked to ensure that DOJ employees and contractors comply with this training.

Users are provided a Privacy Act notice outlined in Section 5.2. General notice to the public is given through JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021) and, DOJ-020, DOJ Identity, Credential, and Access Service Records System, 84 Fed. Reg 60110 (Nov, 7, 2019).

To ensure the continued relevance and effectiveness of security controls, risk assessments, including privacy and security control assessments are routinely evaluated. In accordance with the National Institute of Standards and Technology Special Publication (NIST SP) 800-53 (Rev. 5[4]), these assessments include the management, operational, and technical controls to ensure minimization of any privacy risk.

---

[3] The DOJ Identity and Access Management system (IamDOJ) establishes and maintains the single authoritative source of digital identities for all DOJ employees and contractors. Each person is uniquely represented by an Enterprise Digital Identity (EDI) which enables governance and reporting on identity attributes and permissions. IamDOJ is covered by separate privacy documentation.

[4] NIST 800-53, *Security and Privacy Controls for Information Systems and Organizations,* is available at https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.