Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
DOJ Enterprise Identity Access Management
(IamDOJ)

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

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

Date approved: December 11, 2023

(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 DOJ Enterprise Identity Access Management, known as IamDOJ, utilizes SailPoint IdentityIQ® (IIQ) software, described in more detail below, to create and maintain a master identity repository as the basis for DOJ's enterprise identity management solution. IamDOJ combines user information from various data sources to provide a centralized and authoritative identity governance solution for DOJ employees, detailees, and contractors. The system allows management and staff to monitor and manage user access (e.g., account request, creation, modification, removal; annual account recertification, etc.) across components, business units, and systems. IamDOJ serves as DOJ's central and authoritative Identity Management data repository, as required by Federal law and Office of Management and Budget (OMB) requirements. JMD prepared this Privacy Impact Assessment (PIA) because IamDOJ will collect and maintain personally identifiable information (PII) on DOJ users.

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.

IamDOJ combines user information from various data sources to provide a centralized and authoritative identity governance solution. The system allows management and IT staff to monitor and manage user access to IT systems (for example, account request, creation, modification, removal; annual account recertification, etc.) across components and business units within DOJ. The system is located within the Secure Enclave hosting environment.[1]

IamDOJ utilizes SailPoint's IIQ software, which offers a comprehensive identity platform and governance solution.[2] SailPoint IIQ provides a means to aggregate data from key systems within DOJ, creating a Master User Record (MUR), and establishing an enterprise digital identity for each DOJ User. SailPoint provides a means to manage and report on the users within DOJ, and provides a means for orchestration with applications and systems for account creations, removals, and approvals aligned to the enterprise digital identity. JMD Office of the Chief Information Officer (OCIO) works with components and their applications to enhance the integration of IamDOJ into account management processes.

IamDOJ uses four functional areas to create a unique representation of a person engaged in an online action, generally referred to as a "Digital Identity":

- TRUST: Validates a person's identity and the degree to which he or she has been vetted.

[1] The JMD Secure Enclave is covered by separate privacy documentation. The Secure Enclave PIA can be found at: https://www.justice.gov/JMD_Secure_Enclave_PIA/download.
[2] More information on SailPoint can be found at: https://www.sailpoint.com.

- BEHAVE: Identifies that the person has the proper training for the roles he or she is assigned and that the training is current.
- CRED: Binds a type of credential or authentication mechanism to a Digital Identity established in TRUST with a level of assurance and is used to grant access (physical and logical[3]).
- PRIV: Captures the privileges (level and type of access) associated with the credential and in turn, the privileges assigned to the Digital Identity.

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
X	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	
X	Other (summarize and provide copy of relevant portion)	DOJ Order 0904, Cybersecurity Program (Sept. 2016); OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019); National Institute of Standards and Technology, Special Publication 800-63-3, Digital Identity Guidelines (June 2017)

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

[3] Logical access controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. See NIST 800-53, Rev 5, Glossary p. 407 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

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	Name is derived from any account that contains the user's name, typically JSTARS, USAccess, NFC, or Active Directory.
Date of birth or age	X	A	Place of birth is obtained from USAccess and used to look users up in USAccess.
Place of birth	X	A	This information is obtained from USAccess.
Gender	X	A	This information is obtained from USAccess.
Race, ethnicity or citizenship	X	A	Citizenship is obtained from USAccess.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A	Full Social Security number is required to correlate JSTARS data to the other data within the system.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A	This information is obtained from NFC and could be updated by the user.
Personal e-mail address			
Personal phone number	X	A	This information is obtained from a component's active directory and could be updated by 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			

(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
Employment status, history, or similar information	X	A	Assuming User Status (Separated, Active, Service, Inactive, Pending) would be included in employment status.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A	This information is obtained from the feed from the MDM and/or SPDR.
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	X	A	This information comes from SPDR geographic location data from the device IP.
Biometric data:			
- **Photographs or photographic identifiers**	X	A	This information is from USAccess.
- **Video containing biometric data**			

(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
- **Fingerprints**	X	A	While fingerprints are not within the system, metadata for users (Fingerprint-PrimaryPrintIndicator; Fingerprint-SecondaryPrintIndicator; Fingerprint-FTEReasonCode) are passed from USAccess.
- **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	IamDOJ 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	IamDOJ 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.
- **IP address**	X	A	IamDOJ 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	IamDOJ 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**			

(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
- **Contents of files**			
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		Email			
Other (specify):					

Government sources:					
Within the component	X	Other DOJ components	X	Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Other federal agencies, the General Service Administration and the U.S. Department of Agriculture maintain the USAccess and National Finance Center (NFC) systems, respectively. These systems have automated emails and workflows which are used for on-boarding, off-boarding, and other lifecycle activities. IamDOJ does not control what information is entered in those systems or how those systems communicate to the end user.					

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			X	IamDOJ manages user access, removal, annual account recertification across components. Information can also be accessed through a DOJ Search and Reporting Portal, which has a small administrative user base.
DOJ components			X	IamDOJ manages user access, removal, annual account recertification across components. Information can also be accessed through a DOJ Search and Reporting Portal, which has a small administrative user base.
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.

IamDOJ 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.

Individuals have been notified that the account, audit log, and user records maintained in IamDOJ can be accessed or amended in accordance with DOJ regulations and in accordance with the applicable Privacy Act system of records notices (SORNs): JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 Fed. Reg. 37188 (July 14, 2021), and DOJ-020, DOJ Identity, Credential, and Access Service Records System, 84 Fed. Reg. 60110 (November 7, 2019). Individuals are regularly informed that they have no expectation of privacy and that Department information systems are routinely monitored for IT security and other lawful government purposes through the login banner, annual cybersecurity and privacy training, and the DOJ Cybersecurity and Privacy Rules of Behavior for General Users (acknowledged annually by Department personnel). Where information was collected directly from individuals by DOJ and maintained in JSTARS or LearnDOJ, those individuals were provided Privacy Act § 552a(e)(3) notices.

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 will be no opportunities for individuals to voluntarily participate in the collection of information in IamDOJ. IamDOJ is used for managing user access and accounts from various data sources to provide a centralized identity governance solution. The general information collected and stored in IamDOJ will be account information including, but not limited to, name, date of birth or age, place of birth, gender, race, or ethnicity, or citizenship, Social Security number, personal mailing address, personal phone number, employee status, or history, or similar information, device identifiers, location information, photographs, fingerprints, system admin/audit data (user ID, IP address, date/time of access).

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.

As stated above, individuals have been constructively notified that the DOJ maintains records in IamDOJ by DOJ's publication of JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, and JUSTICE/DOJ-020, DOJ Identity, Credential, and Access Service Records System. Both SORNs detail the process by which a person can access records pertaining to that individual, or amend records that the individual believes are inaccurate, irrelevant, untimely, or incomplete.

Individuals may also follow the procedures outlined on OPCL's website, "Requesting Access to Records in Accordance with the Privacy Act," and "Requesting Amendment or Correction of Records in Accordance with the Privacy Act," at www.justice.gov/privacy, and in Subpart D, Part 16, Title 28, Code of Federal Regulations.

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):** 1/11/21. IamDOJ will move from an ATO to an Ongoing Authorization, which was awarded in January 2021. **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:** None
	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:** IamDOJ conducts vulnerability and configuration scans monthly. The Information System Security Official 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 and will be reviewed by the ISSO on a weekly basis using the Splunk dashboard.
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 the DOJ Cybersecurity and Privacy Rules of Behavior both prior to accessing the DOJ network and annually thereafter. System administrators, including IamDOJ 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 IamDOJ and has been assessed as a High Impact information system. As such, IamDOJ has implemented appropriate security and privacy controls commensurate with such a designation, including logical access, identification and authentication, vulnerability management, and auditing security controls.

IamDOJ 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 are being sent to DOJ's centralized audit log management system for triage and review. The ISSOs are charged with reviewing logins and performing auditing functions to ensure role-based access controls satisfying the above measures.

Because IamDOJ will be maintained within the DOJ Secure Enclave, IamDOJ will also utilize the technical safeguards implemented within Secure Enclave. For example, IamDOJ will use Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2,[4] to protect data in transit. Additionally, IamDOJ utilizes an Application Layer Firewall[5] and integrated Intrusion Detection System / Intrusion Prevention System[6] technology and encapsulates in an Internet Protocol Security Virtual Private Network (IPSEC VPN)[7] all data replication/transit between the two Secure Enclave datacenters. IamDOJ also encrypts data when transmitted. JSTARS is encrypted over Secure File Transfer Protocol (SFTP), USAccess System Infrastructure Provider (SIP) is an encrypted webservice, and NFC is encrypted via internal emails. When the data is at rest, the social security numbers us a secure hash algorithm.[8]

---

[4] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/groups/STM/cmvp/standards.html.
[5] An "Application Layer" firewall is a form of firewall that controls input, output, and/or access from, to or by an application or service.
[6] An Intrusion Detection System (IDS) analyzes and monitors network traffic for signs that indicate attackers are using a known cyber threat. Intrusion Prevention System (IPS) proactively denies network traffic based on a security profile if that packet represents a known security threat.
[7] Internet Protocol Security, or "IPSEC," is "a framework of open standards for ensuring private communications over public networks" and is "typically used to create a virtual private network." NIST SP 800-77, *Guide to IPsec VPNs* (Dec. 2005). A Virtual Private Network, or "VPN," is a "virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks." *Id.*
[8] A secure hash algorithm is a mathematical function that makes data unreadable. These algorithms process a message to produce a condensed representation called a message digest. These algorithms enable the determination of a message's

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 incident. DOJ maintains user audit log data indefinitely and system logs are kept 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, 86 Fed. Reg. 37188 (July 14, 2021).

JUSTICE/DOJ-020, DOJ Identity, Credential, and Access Service Records System, 84 Fed. Reg. 60,110 (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),***

---

integrity: any change to the message will, with a very high probability, result in a different message digest. See https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

- ***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.***

IamDOJ is an identity management software which combines user information from various data sources to provide a centralized identity governance solution for DOJ employees and contractors. IamDOJ collects PII for operational purposes. The PII collected includes name, date of birth, place of birth, gender, citizenship, Social Security number, personal mailing address, personal phone number, user status, device identifiers, location information, photographs, system admin/audit data (user ID, IP address, date/time of access). All data retention is managed according to System Owner requirements and associated policies and is determined on the tool, service, or application level. As much as possible, IamDOJ minimizes the collection of PII; for example, it does not collect certain data types for its users (such as Tax Identification Numbers).

Data sources include USAccess, NFC, JSTARS, component active directories, and LearnDOJ. IamDOJ implements encryption, account management and access controls, and auditing to mitigate and protect personally identifiable information. IamDOJ makes use of separate Privileged and Non-Privileged user accounts; access is granted on least privilege and need-to-know requirements. Users will not be provided an opportunity to voluntarily participate in the collection, use or dissemination of information accessible to IamDOJ Administrators,

Information is shared through direct login access basis within the component, other DOJ components, and other Federal agencies (GSA through USAccess). On top of disk encryption, IamDOJ programmatically encrypts the SSN value in the database using the IamDOJ encryption key, which meets FIPS 140-2 standards. While stored in the system database, SSNs are encrypted as part of the disk encryption provided by the infrastructure in the Secure Enclave environment. While the data is in transit, the flat files are encrypted and software connectors use encryption sufficient to meet FIPS 140-2. The IamDOJ ISSO will also perform 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 IamDOJ, must receive an annual Cyber Security Awareness Training (CSAT). The CSAT course typically includes requirements for proper handling of PII. The course typically 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 the DOJ Cybersecurity and Privacy Rules of Behavior confirming that they have completed this course and that they agree to abide by requirements reviewed in the course and stated in the Rules of Behavior. 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.

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 NIST SP

800-53 (Rev.5), these assessments include the management, operational, and technical controls to ensure mitigation of any privacy risk.