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

Office of Justice Program

Privacy Impact Assessment
for the
Digital Identity and Access Management Directory (DIAMD)

Issued by: Maureen Henneberg

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

Date approved: September 16, 2022

Section 1: Executive Summary

The Digital Identity and Access Management Directory (DIAMD) system serves as Office of Justice Programs' (OJP) Identity, Credential, and Access Management (ICAM) solution. This system allows OJP information technology (IT) staff to monitor and manage external and internal user identities as well as authorize access to OJP information systems. Such activities include, but are not limited to, account requests, creation, modification, removal, and annual account certification. DIAMD provides single identity provider capabilities in accordance with DOJ guidance. DIAMD federates with the Departmental ICAM and aligns with the Office of Management and Budget's (OMB) *M 22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. OJP IT staff use DIAMD to manage internal and external user identities and authorize access to OJP's systems. OJP has prepared a Privacy Impact Assessment for DIAMD because this system collects, maintains, and disseminates Personal Identifiable Information (PII) from internal and external users. The type of information collected is for account management purposes and includes name, contact information, and audit logging information.

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.

OJP relies on its IT systems, including DIAMD, to accomplish its mission of providing cost-effective and reliable services to the Department, other Federal agencies, and the public at large. DIAMD is a managed service offering an Identity-as-a-Service (IaaS) system that delivers a set of identity governance solutions for use by OJP for DOJ users. DIAMD provides identity and access management services for internal and external users for all OJP applications that are integrated with it. OJP's Active Directory is the authoritative source for OJP internal user identity records in DIAMD. DIAMD enables lifecycle management of internal and external users of DOJ organizations that are partnered with OJP.

The solution supports the management of internal users, such as DOJ/OJP personnel and contractors. DIAMD's function is to support user management by adding and removing business roles, managing members, terminating users, resetting passwords, and suspending and unsuspending accounts for OJP internal users. DIAMD is the identity broker gateway for access to OJP managed systems with which it integrates, and it also pushes OJP identity information to the Department's DOJ Login identity broker to provide information to support access of OJP resources to other Departmental systems not directly managed by OJP. The information collected identified in Section I is used to provision accounts for OJP and other DOJ users for identity and access management purposes for systems integrated with DIAMD.

External users of DIAMD are principally grant applicants and grantees. As more systems integrate with DIAMD, external users will expand to include users who have to interface with OJP systems, such as training and training assistance recipients. External users are either invited by the grantee's entity administrator or are registered via self-service with an email address. External users are sent a welcome email and a One Time Password (OTP) so they can create a password. Generally, all information on external users is collected online. However, in some cases users may call the service desk and DIAMD may be updated using that information (after necessary verifications).

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	44 USC 3551 et seq.; 44 USC 3504; and 28 USC 530C
Executive Order	Homeland Security Presidential Directive: Policy for a Common Identification Standard for Federal Employees and Contractors (Aug. 2015)
Federal Regulation	FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors (Aug. 2013)
Agreement, memorandum of understanding, or other documented arrangement	OMB Circular A-130 Managing Information as a Strategic Resource (July 2016); OMB Memorandum M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (July 6, 2010); OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems (Nov. 18, 2013); and OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019).
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). <u>Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.</u>

(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 and C	First and last names of internal and external users. Additionally, usernames may include first initial and last name.
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)	X	C	TINs are collected for individual Grantees as needed by Office of the Chief Financial Officer (OCFO) for payments (not the same as SSN).
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address	X	C	E-mail addresses are collected for external users.
Personal phone number	X	C	Phone numbers are collected for Multifactor Authentication (MFA) purposes for external users.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
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)			
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 and C	Business E-mail address, organization name, and "Doing Business As."
Location information, including continuous or intermittent location tracking capabilities			
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			

(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 (specify)**			
System admin/audit data:			
- **User ID**	X	A and C	User ID
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A and C	Date and time of access
- **Queries run**			
- **Content of files accessed/reviewed**			
- **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	X	Email			
Other (specify): Information will be uploaded into the application.					

Government sources:					
Within the Component	X	Other DOJ Components		Online	
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	Internal users with roles-based credentials have access to information.
DOJ Components			X	DOJ Component users that have been federated via DOJLogin have roles-based access to information. DIAMD shares internal user information with DOJLogin and does not share external user information.
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.

N/A

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.

Pursuant to the Privacy Act of 1974, this system contains records that are maintained by the Department and are retrieved in practice by a personal identifier. As such, the information in this system will require a System of Records Notice (SORN). This System of Records is covered by DOJ-020: DOJ Identity, Credential, and Access Services Records System, which provides a generalized notice to the public. This SORN was published in full at 84 FR 60110 on November 7, 2019. Additionally, OJP is working to add a Privacy Act 552a(e)(3) notice for external users.

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.

The system does not allow for anonymous access. User account information may be shared with individuals in each office on a need-to-know basis. For internal users the information is collected by Active Directory and users are provided a statement clarifying that there will be no expectation of privacy as to the use of Federal government equipment (see Notice at 6.2); when each internal user joins the Department, their information will be collected by their consent. Internal users may consent to the collection, uses or dissemination during self-service registration, although they often are required to provide certain information to be able to use the system to perform their job duties. At the time of this publication, external users are not currently provided with a Privacy Act § 552a(e)(3) Notice. However, OJP is developing this Notice and will implement it expeditiously. Usage of the system is voluntary for external users, however their usage is subject to their consent to the collection of their information.

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 provided in the DOJ SORN that covers the DIAMD system, individuals seeking to contest or amend records must directly contact the Justice Management Division's (JMD) Freedom of Information Act (FOIA) office. Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the "Record Access Procedures" paragraph in the SORN. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked "Privacy Act Amendment Request". All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

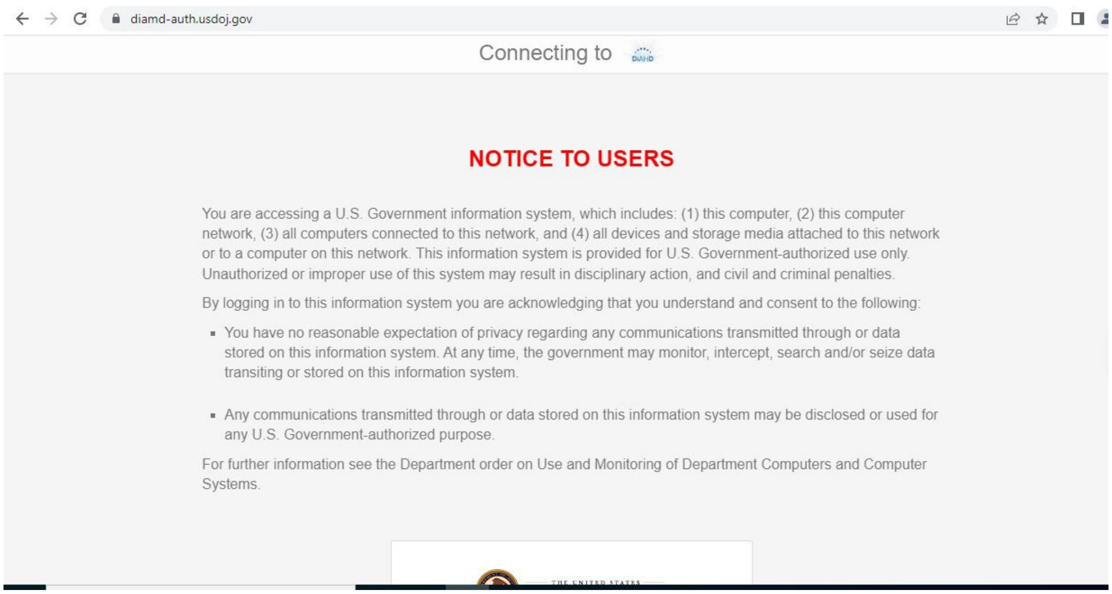
<u>Section 6</u>: Maintenance of Privacy and Security Controls

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):** April 1, 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:** There are no POA&Ms associated with privacy controls.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain: N/A
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DOJ/OJP Cybersecurity Standards and Continuous Monitoring: DOJ's annual Core Control assessment includes the testing and evaluation of the security and privacy controls safeguarding DIAMD information. In addition, DOJ/OJP monitors the monthly continuous monitoring submissions from Cloud Service Providers (CSPs) for all Cloud Service Offerings (CSOs) supporting the DIAMD system in accordance with the Federal Risk and Authorization Management Program (FedRAMP) Continuous Monitoring requirements.
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:** Application audit logs are ingested by Splunk and reviewed in accordance with OCIO 62 Security and Privacy Assessment and Authorization Standard Operating Procedures.
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**.
	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:

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?*

DIAMD provides a Privacy-related warning banner as displayed below:



Additionally, roles are provisioned through automated workflows, and on occasion by an Administrator and are approved by the System Owner to mitigate the chance for unauthorized access.

Lastly, information is encrypted at rest and in transit within the DIAMD system. OJP's Application Programming Interface Management (API-M) secures the transmission of information between the DIAMD solution and the various internal and external components using encryption commensurate with FIPS-199 requirements for a moderate security categorization.

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 National Archives and Records Administration, General Records Schedule 3.2: "Information System Security Records" 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.

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. ☒ 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-020, DOJ Identity, Credential, and Access Services Records System, 84 FR 60110 (11-7-2019).

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.***

In order to mitigate the risk of over-collection of personal information, DIAMD limits the collection of information to those required for identity management purposes and only collects information from internal and external users on an as-needed basis. The personally identifiable information (PII) collected includes name, email address, personal phone numbers for external users for multi-factor authentication purposes, and audit information, and is collected as needed to allow users to perform identity and access management tasks.

Another potential privacy risk arises from potential unauthorized access or use of information. In order to mitigate this, DOJ's Personnel Security Office vets personnel, including full-time employees (FTEs) and contractors with background checks and signed Rules of Behavior (ROB) for General and Privileged Users. To further ensure data integrity, Information Technology and Security Division (ITSD) conducts vulnerability scans and audit reviews in accordance with and documented within DOJ and OJP policy. These guidelines identify the appropriate levels of review as well as adjustments necessary in light of changes in risk. Audit records are processed using a Security Information and Event Management (SIEM) solution analyzing the minimally required audit fields.

Role-Based Privileges are provided to Managers and Contracting Official Representatives to approve roles. DIAMD employs the principle of least privilege and defined roles or groups which can be based on separation of duties (SOD). Least privilege means that users are provisioned with the least amount of access and editing privileges required to perform their role within the system. DIAMD provides lists of users affiliated with approved roles or groups for system owners to enforce least privilege and ensure data encryption.

On DIAMD's login page, users are provided with a notice that they are accessing a U.S. Government information system. By logging into the system, users acknowledge and consent to no reasonable expectation of privacy in communications or data storage on the system. Users are also provided a link to the Department of Justice's (DOJ) Privacy Policy from the login page. When internal users log in, they are routed through a single sign on (SSO) to the DIAMD console. When external users log in, they are asked security questions and routed through multi-factor authentication (MFA), which prompt notifications regarding access granting or denial to the external user. The final stage of the entry process for external users who have applied or been given a grant is the entity administrator's approval of the request. In order to prevent unauthorized access, internal and external users are disabled after OJP's defined time period.

Decisions regarding security and privacy administrative, technical and physical controls over the information are handled by specialist ICAM staff in ITSD. Users of the system gain access to the data with a valid user ID and password, where access to the data in the system is further limited by the user's assigned role within the system. The system leverages FedRAMP compliant cloud service infrastructure with security controls, including physical safeguards appropriate for a FISMA moderate system.