U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: DOIAccess System
Bureau/Office: Office of the Chief Information Officer
Date: June 17, 2022
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☒ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

DOIAccess is the Department of the Interior (DOI) Enterprise Identity Management System. This system creates and maintains identity accounts for all DOI employees, and those contractors and associates (including volunteers) who require access to DOI networks, information systems and regular facility access. DOIAccess helps DOI provide for interoperability and trust in allowing physical access to individuals entering DOI controlled

facilities, and allowing logical access to Federal information systems, networks, and resources. The Identity, Credential and Access Management (ICAM) office within the Office of the Chief Information Officer manages the DOIAccess system.

DOIAccess identity accounts support DOI's mission to issue and manage Personal Identity Verification (PIV) credentials (DOI Access Cards) required by Homeland Security Presidential Directive 12 (HSPD-12) in compliance with Federal Information Processing Standard (FIPS) 201 procedures. In addition, DOIAccess creates standard network and email accounts, and allows DOI to comply with Office of Management and Budget (OMB) Memorandum M-19-11, *Federal Cybersecurity Requirements for Strong Authentication*, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3. DOI Access Cards eliminate the need for lower-level network authentication (username and password) and provides a phishing resistant authentication capability to all DOI standard and privileged network users, as required by OMB M-22-09.

DOIAccess is a Government off-the-shelf system that provides a streamlined, automated and standard process to collect and manage identity and credential (DOI Access Card) information. All DOI Human Resources (HR) or Contract Officer Representative (COR) offices use DOIAccess throughout the employment lifecycle, starting with the on-boarding and adjudication process, updating identity, credential, and adjudication information throughout the employment cycle, and requesting suspension or termination of employment at the end of the cycle. DOI managers can also initiate a DOI Access Card request or employment termination request. DOIAccess is also used during bureau transfers to update the business information to maintain accurate records as personnel change positions within DOI. DOIAccess is considered the authoritative data source for DOI contractor personnel who require a DOI Access Card for network or physical access.

DOIAccess synchronizes digital identity and adjudication data from authoritative data sources: DOI Federal Personnel and Payroll System (FPPS), Active Directory (AD), Financial and Business Management System (FBMS), and the United States General Services Administration (GSA) USAccess system. DOIAccess also ensures synchronization of credential data between USAccess, DOIAccess, AD, and each DOI Access Card, to ensure the DOI Access Cards can be used for access to networks, systems and facilities.

DOIAccess also supports OMB-mandated Continuous Diagnostics and Mitigation (CDM) Program goals by providing identity data to Sailpoint. DOIAccess provides authoritative data for identity, adjudication, and credential data elements required to create and maintain the DOI Master User Record for all employees, contractors, and associates. The Sailpoint system will be assessed in a separate privacy impact assessment (PIA).

C. What is the legal authority?

5 U.S.C. 301, *Departmental regulations*; Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551); E-Government Act of 2002 (Pub. L. 107-347, Section 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork

Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

Below are the applicable Executive Orders, Federal policies and publications for this system:

- Executive Order 13800, *Strengthening the Cybersecurity of Federal Network and Critical Infrastructure* (May 11, 2017)
- Executive Order 13681, *Improving the Security of Consumer Financial Transactions* (October 17, 2014)
- OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022)
- OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* (May 21, 2019)
- OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (August 5, 2005)
- OMB M-05-05, *Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services* (December 20, 2004)
- Homeland Security Presidential Directive 12 (HSPD-12) – *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004)
- NIST SP 800-63-3, *Digital Identity Guidelines* (June 2017)

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☒ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☒ Other: *Describe*

The system moved hosting locations from Reston, VA to USGS Earth Resources and Observation Science Data Center Sioux Falls, SD. The system was modified to streamline data import from FBMS and data sharing with Sailpoint.

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000002258; DOIAccess System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

GSA government-wide system of records notice (SORN), GSA/GOVT-7: HSPD-12, USAccess, 80 FR 64416 (October 23, 2015). This SORN may be at https://www.fpc.gov/resources/SORNs/.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Citizenship
☒ Birth Date
☒ Biometrics
☒ Other Names Used
☒ Legal Status
☒ Place of Birth
☒ Security Clearance
☒ Social Security Number (SSN)
☒ Personal Email Address
☒ Employment Information
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

Federal Emergency Response Official indicator, User Principal Name (UPN), digital facial image, fingerprint, work phone number, work mailing address, work email address, organization code, results of investigation, and PIV credentials and certificates.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

Individual data is submitted by the applicant during the DOI on-boarding process and entered into DOIAccess by Bureau Sponsors or CORs. Results of background investigations are adjudicated by DOI bureaus and offices and recorded in DOIAccess. GSA provides biometric data (photo and fingerprints) collected during the individual's Enrollment appointment at a USAccess Credentialing Center and stored in the USAccess System. The full data set, individual data from DOIAccess, and adjudication and biometric data from USAccess, must be in place to initiate creation of a DOI Access Card.

DOIAccess data such as name, UPN, email address and organization information is shared with DOI AD for the purpose of creating network and email accounts. DOIAccess also validates employee's identity data entered by the Sponsor with FPPS identity data created a few weeks later by DOI HR offices.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☐ Email
☒ Face-to-Face Contact
☒ Web site
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems *Describe*
☒ Other: *Describe*

Paper Format: All new hires submit completed paperwork required for on-boarding, which includes PII and other fields. Once the written data is collected, Sponsors (HR), CORs, supervisors, and network users enter the relevant data into the DOIAccess system

"Request a new Card" screen to initiate the on-boarding process. This information is then sent to the USAccess system.

Face-to-Face Contact: All new hires are required to visit a USAccess Credentialing Center for an Enrollment appointment, where they will verify their identity information uploaded from DOIAccess, and submit the digital collection of their facial image via camera, and fingerprints via an electronic fingerprint device that captures fingerprint rolls and slaps. In addition, they will provide two forms of proof of identity (i.e. driver's license and passport), which are scanned into the USAccess system. The photo and fingerprint data is shared with DOIAccess but the scanned identity documents are only maintained in USAccess.

Website: DOIAccess allows HR Sponsors or CORs to enter data from the paper format during the on-boarding process, or at any time during the employment cycle, as needed, to update the record for name changes, employment status changes, duty station changes or for other card management activities (i.e. re-enrollment).

Information Shared between Systems: DOIAccess shares identity, adjudication and credential information with the following systems:

- USAccess - Sensitive PII data is shared with DOIAccess.
- AD - Non-Sensitive PII data is shared: Employee name, official email address, UPN, credential information, and employment status.
- FPPS - Sensitive PII data is received. DOIAccess receives HR data from FPPS with name, organization, employment status and other HR fields.
- CDM Master User Record - Sensitive PII data is shared with Sailpoint to support the CDM program. DOI sends the Master User Record new and updated name, organization, supervisor, adjudication and credential data.

D. What is the intended use of the PII collected?

Intended use of the PII is to ensure the safety and security of Federal facilities, systems, or information, and of facility occupants and users; to provide for interoperability and trust in allowing physical access to individuals entering Federal facilities; and to allow logical access to Federal information systems, networks, and resources.

DOIAccess collects and maintains PII data for the purpose of completing the Identity Proofing and PIV Credential Issuance in accordance with FIPS 201. Individuals who require regular, ongoing access to Departmental facilities, information systems and networks, and/or information classified in the interest of national security, including applicants for employment or contracts with DOI, Departmental employees, contractors, students, interns, volunteers, affiliates, and individuals formerly in any of these positions. The system also covers individuals authorized to perform services provided in Departmental facilities (e.g., Credit Union, Cafeteria, Cleaning Services, etc.).

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

All DOI-authorized Sponsors, Adjudicators, and CORs have the level of access to bureau/office PII data in DOIAccess appropriate to their official duties. These personnel enter PII data into the system to on-board new applicants, and update data of existing employees, contractors and associates.

Sensitive data is stored in an encrypted database and the data is displayed through a User Interface. Authorized users go through annual training which provides guidelines of how PII data shall be used.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Authorized DOIAccess Sponsors and Adjudicators do not have access to DOI PII data for personnel in other bureaus, unless they have a verified business need to take actions on that bureau's records. This expanded bureau access is limited to one or two personnel per bureau, for the purpose of accessing PII data to initiate a new National Criminal History Check prior to a bureau transfer action. All other Sponsors, supervisors, and CORs using DOIAccess have a limited view of all DOI records, i.e., name, but no other PII.

Details on incidents may be shared with authorized bureau/office officials for collaboration to respond to a data breach and remedial measures, conduct investigations or perform malware analysis. Data may also be used to assist in HR investigations or aid Law Enforcement or Insider Threat Program investigations when there is a potential violation of law, regulation or policy.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Data is shared with the GSA USAccess system to process data during an employee's USAccess Enrollment, to verify the data as part of the required identity proofing process, and to produce a DOI Access Card based on a proven identity, verified PII data, completed background investigation data. Data is also shared with the Department of Defense to perform the National Criminal History Check (NCHC), along with National Agency Check with Inquiries (NACI). The NCHC and the NACI include criminal history checks, employment and educational history verification, residence verification, and reference checks. Data may be shared with other external organizations as authorized under the Privacy Act and outlined in the routine uses in the GSA/GOVT-7 system of records notice, which may be viewed at https://www.fpc.gov/resources/SORNs/.

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☒ Contractor: *Describe the contractor and how the data will be used.*

Data may be shared with DOI contractors under contract to provide support to the DOIAccess system. Data is also shared to support yearly DOI FBMS Financial Audits on behalf of the DOI Office of Inspector General (OIG). Typical data to be shared includes legal name, employment status, termination date, and network account disabled date. The data is used to verify if employees or contractors who are no longer active employees of the Department can still access financial applications.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

All information provided by individuals is voluntary as a condition of employment and a prerequisite for accessing DOI facilities and computer resources. Individuals may decline to provide information required during the enrollment process; however, failure to provide the requested information would prevent the agency from completing a background investigation and prevent the applicant from obtaining a DOI Access Card needed for access to DOI networks and facilities. A Privacy Act Statement is provided at the time of presentation of PII data during the enrollment appointment. Also, various Federal HR standard forms completed by applicants contain Privacy Act Statements that inform individuals of the uses of their PII and the consequences of not providing requested information.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is displayed on the home screen of the DOIAccess system. All personnel entering data, including PII data, must accept this statement prior to being granted access to records. PII data is entered by a DOI Sponsor prior to the on-boarding process.

GSA provides a Privacy Act Statement to individuals during the enrollment appointment at USAccess enrollment centers.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through the publication of this PIA and GSA/GOVT-7: HSPD-12, USAccess, 80 FR 64416 (October 23, 2015).

☒ Other: *Describe each applicable format.*

All users are provided with a Privacy Notice that warns of the privacy requirements, consent to monitoring, and references the DOI Privacy Act regulations and applicable Privacy Act penalties when accessing the DOIAccess system or the DOI network.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Authorized Sponsors may retrieve a single record (one identity) by using one of the following search features: name, Social Security number (SSN) and date of birth, person ID, or by email or UPN.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

DOIAccess has multiple automated reports available to DOIAccess Sponsors and people assigned report access. These reports contain names but do not have any sensitive PII data. Below is a description of the reports and the individual data that can be pulled from each report.

- Combined Applicant Status Report - large data file showing the status of a person going through the four processes to be issued a DOI Access Card: Sponsorship, Enrollment, Adjudication, and Card Activation. This report is used by the bureaus to identify personnel who may be stuck in some part of the card issuing process.
- Active Directory Snapshop - a current file from DOI's AD containing name, email, UPN and other AD attribute data. This report is used to get a quick look at the AD data used by DOIAccess, without having to look it up record by record.
- Separation Report - a current file from DOIAccess showing name, organization information of all personnel who have been suspended or terminated from employment with DOI. This report also includes the names and organization information for personnel with name, affiliation or bureau changes for the previous 30 days. This report is used by system owners to search their own system roles and remove any personnel who have separated from DOI or transferred to another bureau.
- Role Assignment Report - a current file displaying name, system role, bureau/sub-bureau access assigned, email, and person identifier. This report is used by bureaus and offices to audit role assignments.

- Affiliation Change Report – displays affiliation changes between the Employee, Contractor or Associate
- Invalid Sponsor Report – identifies records that do not have a valid sponsor managing that record
- Upcoming Card Actions Report – identifies records that have some type of upcoming actions on their DOI Access Cards
- Duty Station Report – used to validate duty station data
- Electronic FOIA Tracking System Submission Report – displays current requests for fingerprint checks
- Organizational Personnel Report – displays personnel by organization code
- Card Reissue/Renewal Report – displays cards requiring a reissue or renewal by date

In addition to the DOIAccess Sponsors, these reports are also available to the OIG and the IT Security office for investigative purposes. Data may also be reviewed to "troubleshoot" issues, such as determining why a DOI Access Card has not printed, or why the DOI Access Card certificates are not functioning.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data collected from sources other than DOI records is processed through automatic data validation checks in DOIAccess. These checks will identify duplicated data or potential discrepancies with existing data and any discrepancies are displayed in a DOIAccess discrepancy queue. Certain information such as name and SSN are verified during the background check and verification process. Discrepancies are manually reviewed and verified for accuracy, and incorrect records are updated to ensure records are current and accurate. All employees, contractors, and associates have access to view their own personal identity information contained in DOIAccess and can follow the outlined process to contact their Sponsor if any information needs to be corrected.

B. How will data be checked for completeness?

DOIAccess has required fields that must be entered to complete an identity record on an individual. A Sponsor entering an applicant data must certify they have verified the accuracy of all PII and other data against the applicant's paperwork before they can save the record. All employees, contractors, and associates have access to view their own personal identity information contained in DOIAccess and can follow the outlined process to contact their Sponsor to ensure their information is complete.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

The accuracy of identity data is critical for DOI and must be maintained to ensure the identity value information is updated as needed. Therefore, there are two processes for updating data, manual and automated data updates.

Manual:

- DOIAccess Sponsors and CORs are required to ensure the data is current in DOIAccess. Sponsors and CORs must follow procedures to maintain current data changes that occur after the initial record creation, such as, name changes, organization data changes, affiliation changes or employment status changes. Required changes are received in three ways: the applicant notifies the Sponsor or COR that their personal information has changed (name change); HR documentation (SF-52s) or contract changes are provided to the Sponsor; or updates from other official data sources.
- All employees, contractors, and associates have access to view their own personal identity information contained in DOIAccess and can update home address information and verify other identity attributes. If needed, they can follow the outlined process to contact their Sponsor to update their information.

Automated Data Updates: Systems designated as the sources of identity information provide automatic data updates in the form of a data view, shared data file, or data transaction through interfaces. FPPS (HR), USAccess, AD (IT) and FBMS (COR and Facility) data is received into DOIAccess to automatically update identity attribute data, ensuring the data in the system is always current. The DOIAccess Database Models document identifies the information that is automatically updated from each of these sources. Additional information regarding imports can be found in the DOIAccess System Documentation folder and DOIAccess Web Application technical document.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Records maintained in DOIAccess are subject to the disposition authorities under the Departmental Records Schedule (DRS) DAA-0048-2013-0002- Long-term Administration Records, as approved by the National Archives and Records Administration (NARA). Records under this category include personnel credential files and current building access files (employee identification cards or rosters showing current security clearance status of individuals). The records disposition is temporary and records are destroyed 7 years after cut-off when employee or contractor separates or is no longer employed by the agency. PIV identification cards and related documents are authorized for destruction under DAA-0048-2013-0001-0002-0003, Administration Records of Specific Temporary Value, and will be destroyed 90 days after the card is returned to the issuing office.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

DOIAccess data for applicants that are permanently separated or no longer under contract are maintained with active records. PIV cards, DOI Access Cards are destroyed by shredding the card in accordance with FIPS 201-2 upon return of the card during the off-boarding process.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a privacy risk to individuals in the DOIAccess system due to the volume of sensitive PII maintained in the system. Information collected and maintained in DOIAccess is required as part of the DOI on-boarding process to verify identity, employment eligibility, and issue PIV cards. DOIAccess maintains a single identity account that links an individual to their background investigation results including creation of a standard DOI network and email account. DOIAccess is a Federal Information Security Modernization Act (FISMA) Moderate system that requires management, operational, and technical controls established by NIST SP 800-53 to mitigate privacy risk for unauthorized access or disclosure of PII that may lead to identity theft, fraud, and exposure of sensitive information. DOIAccess has undergone a formal Assessment and Authorization for issuance of an authority to operate in accordance with FISMA and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system. As part of the continuous monitoring program, continual auditing will occur on the system to identify and respond to potential impacts to PII information stored within DOIAccess.

There is a risk of unauthorized access to the system, exposure, loss or compromise of PII. This risk is mitigated by security and privacy controls implemented to safeguard the information in the system. All internet connections with subscribing systems are NIST FIPS 140-2 compliant and encrypted point-to-point data transmission. Operational and technical controls in place include firewalls, malware identification, and periodic verification of system users, in addition to physical controls. Information is used, retained, and processed by authorized personnel based on need-to-know and least privilege principles. Users are assigned least privileges access to accomplish their job duties. DOIAccess is an internal system that may only be accessed from within the DOI network with the proper credentials. All system users must use PIV authentication to access the DOIAccess system and users will have restricted access to resources based on their role. System logs track authorized users' access to and actions within the system. Authorized users are identified by their unique applicant ID, and their actions within DOIAccess are monitored through the application audit trail. Access to administrative functions such as audit logs and monitoring is strictly controlled. Only administrators and personnel with an official "need to know" can perform these functions. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, and criminal, civil, and administrative penalties.

Developers must have administrative accounts to access DOIAccess servers. Physical access to the servers that host DOIAccess is restricted through limited access to the secure DOI data center. In order to access the data center, personnel require a keycard or must be escorted by personnel with a keycard. Data centers are monitored via Closed Circuit Television and all entry is logged through visitor and card access logs. Data collected through paper format during the application process (on-boarding process) is strictly controlled and limited to authorized personnel who require access to perform their official duties and specified as to the level of access within each bureau/office.

There is a risk that the individual may not have adequate notice or have the opportunity to consent to the uses of their information once it is collected. This risk is mitigated through the Privacy Act Statement provided to individuals on the DOIAccess home screen and at USAccess enrollment centers, Privacy Act Statements provided through various HR forms during the on-boarding process, publication of this privacy impact assessment, and the published GSA/GOVT-7: HSPD-12, USAccess, SORN.

There is a risk that information in the DOIAccess system will be maintained longer than necessary to achieve the agency's mission, or that records may not be properly destroyed. This risk is mitigated by managing records in accordance with a NARA-approved records schedule and providing extensive training to users on IT security, Privacy, Records Management and Controlled Unclassified Information (CUI). The System Owner will work with DOI records officials to ensure records in the system are properly maintained and disposed of to mitigate privacy risk.

There is a risk that PII may not be accurate. DOIAccess has data validation checks in place to identify any discrepancies such as incomplete or duplicated data. All system users have access to view their own personal identity information in DOIAccess and can follow outlined processes to contact their Sponsor if any information needs to be updated or corrected.

There is a risk that PII may be misused or used for unauthorized purposes. DOI authorized personnel signs the DOI Rules of Behavior (ROB) and are subject to monitoring in the system and DOI network. All employees and contractors must complete Information Management and Technology (IMT) awareness training, which includes cybersecurity, privacy, records management, CUI, Section 508, and the Paperwork Reduction Act prior to being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities, such as law enforcement personnel, must also take role-based privacy training (RBPT) initially and annually, to ensure an understanding of the responsibility to protect privacy.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

DOIAccess is designed to manage identity accounts to issue PIV credentials in accordance with the requirements of HSPD-12 and FIPS 201-2. Only the data needed for this purpose is included in DOIAccess. While DOIAccess stores a significant amount of PII, all PII stored is needed in order to properly ascertain an individual's identity.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable. No new data is created, and therefore will not be verified for relevance or accuracy.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☐ System Administrator
☒ Other: *Describe*

DOIAccess role holders: System Admin, Sponsors, Adjudicators, AD Administrators, Card Managers, Security, Print Operator and Report Viewer. In addition to these official roles, all users have access to see their own complete record, including their own PII data, and update their home address data.

All users can search for and open a record for any other individual (employee, contractor, or associate), but that user will only see official work related information such as name, PIV credential issuance status, identification data (UPN, Person ID, email, bureau and network domain), business information (DOI organization, duty station, supervisor name), and PIV credential information (card expiration, certificate expiration, and other data related to the PIV process - sponsorship, enrollment, and issuance.

Contractors working for DOI fall into the same category as "All Users". Developers on the DOIAccess system, who are also contract staff, have full access to the data repository. Developers must complete IMT and Computer Security Incident Response Team (CSIRT) annual training and sign ROB to obtain Administrative Accounts and access to DOIAccess servers.

DOIAccess role holders have specific access as follows:

- System Admin - Access to all records in the system
- Sponsor - Sponsor role access to supported Bureau(s)/Sub-Bureau(s) records only
- Adjudicator - Adjudicator role access to Bureau(s)/Sub-Bureau(s) records only
- AD Administrator - View only access to Bureau/Sub-Bureau records only
- Card Managers – Limited access to manage PIV cards for their Bureau/Sub-Bureau only
- Security – View access to support law enforcement investigations
- Print Operator – Support local printing, can view queue of records
- Report Viewer – Access to download DOIAccess reports for their Bureau(s)/Sub-Bureau(s).

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Role requests are submitted by designated Bureau/Office ICAM Leads. All requests for role-specific access are approved by the ICAM Project Management Office. The Sponsor and Adjudicator roles require proof of completed training from both the DOIAccess and USAccess system. Other roles require proof of completion of DOIAccess training in DOITalent.

DOIAccess Sponsor and Adjudicator role holders must maintain an active corresponding Sponsor and/or Adjudicator role in the GSA USAccess system, and they must complete the annual RBPT training in DOITalent. A user's least privilege and official need to know determine the level of access a user is granted.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Yes, the application design, development and the maintenance are handled by contractor staff and Privacy Act clauses were inserted into their contract. The contractors working on DOIAccess systems shall go through Level 5 Moderate Risk Background Investigation (MBI) background check and shall obtain Administrator accounts to be able to access the servers.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The DOIAccess system will provide the capability to identify, locate, and monitor PIV card applicants and PIV card holders whose information is contained in the system. The system logs authorized users' access to this data, such as system administrators, and tracks their actions within the system.

Authorized users are identified by their unique applicant ID and their actions within DOIAccess and monitored through the application audit trail.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

All access to the system and actions by authorized users within DOIAccess can be reviewed for auditing purposes. Audit reports are customizable and may include, but are not limited to, unique applicant ID logon/logoff timestamps; data accessed and/or modified; and permission changes.

M. What controls will be used to prevent unauthorized monitoring?

Access to administrative functions such as audit logs and monitoring is strictly controlled. Only administrators and personnel with an official "need to know" can perform these functions.

All users must complete IMT awareness training and acknowledge the ROB before being granted access to any DOI IT resource, and annually thereafter. System administrators and security personnel with access to DOIAccess records have additional role-based training requirements.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. *Describe*

Personnel must use a keycard to access the data center or escorted by personnel with a keycard.

(2) Technical Controls. Indicate all that apply.

☐ Password
☒ Firewall

☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The ICAM Program Manager within the Office of the Chief Information Officer serves as the DOIAccess Information System Owner and the official responsible for oversight and management of the DOIAccess security controls and the protection of agency information processed and stored in DOIAccess. The Information System Owner, Information System Security Officer, and authorized bureau/office system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in DOIAccess, and addressing Privacy Act requests for notification, access, amendment, and complaints in consultation with DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The DOIAccess Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The DOIAccess Information System Owner and Information

System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with DOI Privacy Officials.