US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/06/2025

OPDIV:

NIH

Name:

ArcID Fingerprint Transmission System (ArcID FTS)

PIA Unique Identifier:

P-2941873-675070

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The PIA has been updated to meet the requirements of Executive Order - Defending Women From Gender Ideology Extremism And Restoring Biological Truth To The Federal Government.

Describe the purpose of the system.

The ArcID Fingerprint Transmission System (ArcID FTS) collects and transmits applicants' fingerprints and associated biographical data to the Defense Counterintelligence and Security Agency (DCSA) for processing.

The ArcID FTS, formerly known as WEBS (Web Enrollment Biometric Solution), is a browser-based biometric enrollment solution used by the NIH Division of Personnel Security and Access Control (DPSAC) to capture and transmit fingerprints to DCSA. ArcID FTS uses a web-based approach for the consolidation and management of biometric data, which centrally stores, monitors, edits and manages the life cycle of a biometric submission record. By collecting information in one secure,

centrally managed location, distributed workstations are not required to keep sensitive data on local or unsecured equipment.

On the back-end, ArcID FTS receives the properly formatted files, then manages and executes transmissions protocols, routing the files through an unidirectional virtual private network (VPN) tunnel to a secure web interface to DCSA.

Describe the type of information the system will collect, maintain (store), or share.

The ArcID FTS collects and maintains user information for identification and authentication purposes, specifically, usernames (used for application login purposes); applicant personal information (last name, first name, middle name, Maiden Name, aliases), social security number (SSN), date of birth, place of birth, occupation, country of citizenship; physical description (sex, demographic information, eye color, hair color, height, weight); address (both employer and address, residential address) and DCSA transmission record. The collection of Personally Identifiable Information (PII) data is submitted to DCSA to process a Special Agreement Check (SAC), which is a criminal history check.

ArcID FTS stores the fingerprints for 30 days after transmission to DCSA. Fingerprints are stored to ensure that transmission is accepted and no resubmissions are needed. ArcID is setup to auto-purge the records on a rolling 30 day basis.

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network, assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The ArcID Fingerprint Transmission System (ArcID FTS) collects and transmits applicants' fingerprints and associated biographical data to DCSA for processing.

The ArcID FTS (formerly known as WEBS) is a browser-based biometric enrollment solution used by DPSAC to capture and transmit fingerprints to DCSA. ArcID FTS uses a web-based approach for the consolidation and management of biometric data, which centrally stores, monitors, edits and manages the life cycle of a biometric submission record. By collecting information in one secure, centrally managed location, distributed workstations are not required to keep sensitive data on local or unsecured equipment.

On the back-end, ArcID FTS receives the properly formatted files, then manages and executes transmissions protocols, routing the files through a VPN tunnel to a secure web interface to DCSA.

The ArcID FTS collects and maintains user information for identification and authentication purposes, specifically, user names (used for application login purposes); applicant personal information (last name, first name, middle name, aliases, SSN, date of birth, place of birth, occupation, country of citizenship); physical description (sex, demographic information, eye color, hair color, height, weight); address (both employer and address, residential address) and DCSA transmission record. The collection of PII data is submitted to DCSA to process a SAC, which is a criminal history check.

ArcID FTS stores the fingerprints for 30 days after transmission to DCSA. Fingerprints are stored to ensure that transmission is accepted and no resubmissions are needed. ArcID is setup to auto-purge the records on a rolling 30 day basis.

Users log in to this system using the IAM Services which maintains its own PIA on record, including all legal authorities documented. The purpose of the IAM Services is to authenticate and authorize all users and computers in a Windows domain type network, assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Date of Birth
Name
Biometric Identifiers
Mailing Address
Place of Birth, Country of citizenship
Physical description (sex, demographic information, eye color, hair color, height, weight)
Occupation
Defense Counterintelligence Security Agency (DCSA) transmission record

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The primary purpose of the PII use is for the transmission of fingerprints to DCSA to conduct the SAC, which is a criminal history check.

Describe the secondary uses for which the PII will be used.

There is no secondary use of the PII.

Identify legal authorities governing information use and disclosure specific to the system and program.

5 U.S.C. 3301, 3302, 7301; Executive Order 10577; Executive Order 11222; Executive Order 12968

Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors., Aug. 27, 2004; Federal Property and Administrative Act of 1949, as amended

5 U.S.C. 301; Information Technology Management Reform Act of 1996 (Pub. L. 104-106, sec.

5113); Electronic Government Act (Pub. L. 104- 347, sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. ch. 35); Government Paperwork Elimination Act (Pub. L. 105-277, sec. 1701, 44 U.S.C. 3504)

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

OPM GOVT-9: File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay

OPM Central 9: Personnel Investigations Records.

NIH proposes to establish a new System of Records (SORN) 09-25-0224, NIH Division of Police

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within the OPDIV

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB 1615-0047, Employment Eligibility Verification: 07/31/2023

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Memorandum of Understanding (MOU) between DCSA and DPSAC. Completed DCSA background investigation files are transmitted unidirectionally through an encrypted tunnel establishing a system-to-system connection with DPSAC.

Describe the procedures for accounting for disclosures.

DPSAC and DCSA conduct periodic internal and external audits of the Information Technology (IT) systems to identify and mitigate vulnerabilities. DPSAC maintains audit logs of the ArcID FTS system and conducts a periodic audit every 30 days. Additionally, receipts for each record transmitted to DCSA and corresponding confirmation are maintained within the ArcID FTS system and reviewed daily. Any record disclosures to an authorized entity are maintained by the System Owner and the DPSAC Director. Production application systems and data are protected by a robust disaster recovery plan. A test of this plan is conducted annually to ensure its effectiveness, test new capabilities, reveal weaknesses, keep IT staff and customers familiar with disaster recovery procedures, and to verify that all disclosures were authorized.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Notification to individuals that their information will be collected and how their information will be used is provided via the instructions, privacy act statements, and routine use statements on official DPSAC collection forms as well as posted documents within the DPSAC office. These official forms provide notification, privacy act statements, and routine use statements to inform the individual how their personal information will be used and why it is needed. The forms also require the individuals consent via signature in order to authorize the collection or release of any personal information.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Individuals can decide to not include PII on the evidence-informed decision making (EIDM) application, however they will not be processed for NIH employment.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

The collection and use of information gathered from system interfaces and manually entered into ArcID FTS by the staff is required as part of the job application and background investigation processes. Notice of information collection is given at the time of applying for and acceptance of employment at the NIH. Individuals can choose to not give their information by not applying for a job position.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Individuals may write, email, or appear in person to the DPSAC. The inquiry must contain the affected individual’s full legal name, a copy of a Form I-9 [Form I-9 is required to confirm the identity of a new employee and eligibility for employment in the United States according to the United States Citizenship and Immigration Services(USCIS)] identifying document and the reason for concern. The issue will be investigated, and the results of the investigation will be provided in writing to the concerned individual.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Periodic audits are conducted to ensure the integrity, availability, accuracy and relevancy.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

ArcID FTS users are vetted and approved for access to PII based upon functional role and suitability tier. All requests for access go through the system administrator.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Determinations conform to role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount

of PII necessary to perform their job.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel (employees and direct contractors) who use NIH applications must complete security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

All users receive in-person training on how to operate the system during the registration process.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are maintained within The ArcID Fingerprint Transmission System in accordance with the following NIH record retention schedules:

Item: 09-422. Personnel security investigative reports. Personnel suitability and eligibility investigative reports.
Personnel security investigative reports. Personnel suitability and eligibility investigative reports. Investigative reports and related documents agencies create or use to support initial favorable eligibility determinations, fitness determinations, and periodic reinvestigations, or to implement a continuous evaluation program.
Disposition: Destroy in accordance with the investigating agency instruction. DAA-GRS-2017-0006-0022

Item: 09-423. Personnel security investigative reports. Reports and records created by agencies conducting investigations under delegated investigative authority.
Personnel security investigative reports. Reports and records created by agencies conducting investigations under delegated investigative authority. Investigative reports and related documents agencies create or use to support initial favorable eligibility determinations, fitness determinations, and periodic reinvestigations, or to implement a continuous evaluation program.
Disposition: Destroy in accordance with the investigating agency instruction. DAA-GRS-2017-0006-002

Records maintained in system of records 09-25-0224, NIH Police Records are currently unscheduled and will be retained indefinitely until authorized for disposition under a schedule approved by the National Archives and Records Administration.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Physical Controls: The IT hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose access is monitored by

locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware