National Aeronautics and Space Administration

Privacy Impact Assessment (PIA)

PIA Entry Name: Remote Enrollment Service

Enterprise Applications Management Office

NASA Point of Contact: Whitney Craig

Phone Number: 256.544.1573

E-mail: whitney.b.craig@nasa.gov

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

The National Aeronautics and Space Administration (NASA) Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) NASA collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. NASA publishes its PIAs, as well as its System of Records Notices (SORNs), on the NASA public-facing website, which describes NASA's activities that impact privacy, the authority for collecting personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

Reviewing Official: Stayce Hoult, Chief Privacy Officer

System Overview:

Remote Enrollment Service is a 3rd party Software as a Service (SaaS) solution managed by Idemia USA and hosted on Amazon GovCloud. The Remote Enrollment Service provides NASA with a solution to meet Federal Processing Standard (FIPS) 201-3, Identity Assurance Level 2 (IAL2) for remote or in-person identity proofing which is required as part of the Personal Identity Verification (PIV) of Federal Employees and Contractors.

Privacy / Authorities and Other Requirements	
List all legal authorities and/or agreements that permit the collection of privacy information by the project. Explain how these authorities permit the project and the collection of privacy information. If the project collects Social Security numbers, also identify the specific statutory authority allowing it.	Social Security Act (42 U.S.C. § 405 (c) 2 (C) (i)) NIST Digital Identity Guidelines (Special Publication 800-63 Suite) FIPS 201-2 Personal Identity Verification of Federal Employees and Contractors M-05-24 "Implementation of Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors" M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 Policy for a Common Identification Standard for Federal Employees and Contractors M-16-04 "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government" M-19-17 "Enabling Mission Delivery through Improved Identity, Credential and Access Management"
The records in the system are covered by an existing published System of Records Notice (SORN).	Existing SORN applicable
The SORN Name and Number.	The following SORN applies: NASA 10SECR: https://www.nasa.gov/nasa-privacy-act-system-of-records-notices-sorns/

Privacy Act of 1974 / Uses of the Information	
Records on individuals are or will be routinely retrieved from the system by using individual's name or other unique identifier (e.g., personal account number, UUPIC, SSN, etc. is used to locate information about an individual in the application/website/information system/paper record).	Yes

Paperwork Reduction Act / Characterization of the Information	
The record/application/website/information system collects information in a standard way (via forms, surveys, questionnaires, etc.) from 10 or more persons (e.g., members of the public and NASA contractors, and grantees).	Yes

Paperwork Reduction Act / Authorities and Other Requirements	
There is an OMB Control Number.	Yes
The OMB Control Number.	OMB# 2700-0158 Expiration Date: 02/28/2026

Privacy / Characterization of the Information	
Information is collected on the following:	NASA Contractors Government Employees Other Business Partners/Contracts, Grantees (including, but not limited to federal, state, local agencies)
Collection contains the following:	Name Date of birth SSN Biometric identifier (fingerprint or voiceprint) Other PII not listed above Passport number Driver's license number Work phone number Work cell phone number Personal cell phone number UUPIC Agency User ID (AUID) Work e-mail address Personal e-mail address Home mailing address Birth certificate Legal documents (divorce decree, criminal records, etc.) Photograph Work Mailing Address Home Phone Number
The collection is the minimum necessary to accomplish the purpose of the collection.	Yes
Discuss the intra-Departmental sharing of information. Identify and list the name(s) of any components or directorates within the Department with which the information is shared.	There is no intra-departmental sharing of information going to or coming from Remote Enrollment Services application.

Privacy / Uses of the Information

NASA will use the information in the following ways:	Collected PII is used to validate the user's identity when verifying eligibility to access NASA systems.
The application/website/information system stores, collects, or maintains Information in Identifiable Form (IIF).	Yes

Consent / Notice	
Does the project provide individuals notice prior to the collection of information?	Yes
If no, explain why individuals are not notified prior to collection of information.	
If yes, describe how the notice provided for the collection of information is adequate to inform those impacted.	Within the application, the enrollee is notified of the types of PII being collected and the reason for its collection prior to enrollment via consent screens.
Do individuals have opportunities to decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If this is not an option, explain why not.	Users would not use the application for enrollment and contact NASA for any next steps to support in person enrollment.
Do individuals have opportunities to consent to specific/targeted uses of their information?	No
If yes, describe the process. If this is not an option, explain why not	Per the design of the application and the consent language, the collection and use of the NASA enrollee information has been restricted to only what is necessary to prove an IAL-2 compliant identity.
The IIF is collected	Voluntary
There is a process in place for the following:	
Ensuring consent is obtained from the individuals whose IIF is stored, collected, or maintained.	Yes
Are individuals provided with notice that they have opportunities to consent to uses, decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If no, explain why not.	Enrollees are given a consent screen in the beginning of the application outlining consent for the collection and processing of their PII and limitations should they decline or opt out.
Are individuals notified of the consequences of providing information?	Yes
If yes, describe the process. If no, explain why not.	Enrollees are given a consent screen in the beginning of the application outlining consent for the collection and processing of their PII and limitations should they decline or opt out.

Data Retention	
Explain how long each type of information is retained. Include a justification for the retention period of each information type and how/why that period is necessary to the mission/project.	Information can be retained within the application for a configurable amount of time based on NASA requirements. Once an enrollment is completed and sent to NASA, all PII undergoes crypto-shredding to remove PII from the Idemia environment. Per the *NRRS 1441.1* The NASA Records Retention Schedule and *SORN 10SECR,* Personnel Security Records are maintained in Agency files and destroyed upon notification of the death or within 5 years after separation or transfer of employee or within 5 years after contract relationship expires, whichever is applicable in accordance with NASA Records Retention Schedules (NRRS), Schedule 1 Item 103. Personnel Security Records are compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information have been exempted by the Administrator under 5 U.S.C. 552a(k)(5) from the access provisions of the Act. The Personal Identity Records are maintained in Agency files and destroyed upon notification of the death or within 5 years after separation or transfer of employee or within 5 years after contract relationship expires, whichever is applicable in accordance with NRRS, Schedule 1 Item 103. Visitor files are maintained and destroyed in accordance with NRRS, Schedule 1 Item 114. Personal Identity Records are compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information have been exempted by the Administrator under 5 U.S.C. 552a(k)(5) from the access provisions of the Act.

Information Sharing	
Is information shared outside of the organization as part of the normal agency operations?	Yes
Identify who the information is shared with, how the information is accessed, and how it is to be used.	Information is shared with Idemia, and potentially the American Association of Motor Vehicle Administrators (AAMVA) and Experian solely to confirm the enrollee's identity to an IAL-2 compliant level.
Describe how the external sharing noted in the previous question is compatible with the SORN noted in PIA-02.	Per SORN 10SECR "To provide relevant information to an internal or external organization or element thereof conducting audit activities of a NASA contractor or subcontractor."

	Record Source Categories: Information is obtained from a variety of sources including the employee, contractor, or applicant via use of the Standard Form (SF) SF–85, SF–85P, or SF–86 and personal interviews; employers' and former employers' records; FBI criminal history records and other databases; financial institutions and credit reports; medical records and health care providers; educational institutions; interviews of witnesses such as neighbors, friends, coworkers, business associates, teachers, landlords, or family members; tax records; and other public records. Security violation information is obtained from a variety of sources, such as guard reports, security inspections, witnesses, supervisor's reports, audit reports.

Redress	
What are the procedures that allow individuals to access their information?	Users have access to the identity viewer in IdMAX and personnel information can be updated via id.nasa.gov. Additionally users may redress information in accordance with instructions found in 10SECR via the Privacy Act.
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	NASA has an exception workflow that will be followed to correct any information or process enrollee's who do not pass the verification checks. Additionally users may redress information in accordance with instructions found in 10SECR via the Privacy Act.
How does the project notify individuals about the procedures for correcting their information?	NASA will adjudicate based on information received from the application. Additionally users may redress information in accordance with instructions found in 10SECR via the Privacy Act.

Auditing and Accountability	
How does the project ensure that the information is used in accordance with stated practices in this PIA?	There is an annual Certificate & Accreditation (C&A) on the Remote Enrollment Services (RES) application where all National Institute of Standards and Technology (NIST) 800-53 controls are investigated and validated. Idemia collects all audit logs from RES which are recorded and maintained for the length of time per NASA policy stated in ITS-HBK-2810.16-01, Audit and Accountability. NASA, EAST2, and Idemia maintain regulatory documents established between NASA ICAM and Idemia that govern use of information, including the Requirements Definition Document (RDD),

	Memorandum of Understanding (MOU) and the Interconnection Security Agreement (ISA).
Describe what privacy training is provided to users either generally or specifically relevant to the project.	Idemia conducts annual privacy training for all employees on proper handling and disposal of all sensitive information including PII. Idemia also maintains companywide policies related to collecting, sharing, processing, and disposal of all information, including PII. Cybersecurity and Privacy Awareness training is required for all NASA users, to include the system administrator. Specific Role Based Training is required for certain roles.
What procedures are in place to determine which users may access the information and how does the project determine who has access?	NASA will identify internal admin users who will have access to the system and grant access to specific Idemia personnel for maintenance purposes. Enrollees will only have access to the system when they are performing an enrollment.
How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within the department and outside?	All agreements are governed by the existing contract, Memorandum of Understanding (MOU) and Interconnection Service Agreement (ISA) . Any changes are discussed with NASA and mutually approved.

Security Controls / Characterization of the Information	
Monitor and Response to privacy and/or security incidents policies.	Yes

Security Controls / Auditing and Accountability	
Technical controls (safeguards) are in place to minimize the possibility of unauthorized access, use, or dissemination of the IIF in the application/ website/ information system/ cloud system.	Yes
Access controls.	Yes

Information Sharing Practices / Characterization of Information	
The application/website/information system/cloud systems collects IIF from other resources (e.g., databases, websites).	Yes
The application/website/information system/cloud system populates data for other resources (e.g., databases, websites, or external agencies, people, or organizations).	Yes

Accessibility, Redress, Complaints / Characterization of the Information

There is a process in place for periodic reviews of IIF in the system to ensure data integrity, availability, accuracy, and relevance.	Yes

Web Measurement and Customizing Technology / Characterization of the Information	
The Application/Website/Information System Utilizes Web Measurement and Customization Technology (Cookies/Persistent Tracking).	No

Agency Privacy Manager (APM):

Guerin, Michael D
HARRIS HOULT, STAYCE D
Kostka, Paul A
Midulla, Laura P
Montasser, Ali S
Scholz, Matthew C
zzzINACTIVE20250402 - Hill, Debra A

APM Review Decision: Concur

APM Review Date: 12/19/2024

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 03/03/2025

STAYCE HARRIS HOULT

Digitally signed by STAYCE HARRIS HOULT
Date: 2025.05.14 09:44:58 -05'00'

CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Witt, Michael

SAISO Review Decision: Concur

SAISO Review Date: 03/14/2025

NASA Senior Agency Official for Privacy (SAOP):

SEATON, JEFFREY M

SAOP Review Decision: Approve

SAOP Review Date: 04/08/2025