National Aeronautics and Space Administration

# Privacy Impact Assessment (PIA)

**PIA Entry Name:** Identity Management and Account Exchange (IDMAX) contains NASA Access Management System (NAMS)

Enterprise Applications Management Office

**NASA Point of Contact:** Birchmeier, Robert

**Phone Number:** 256-961-2377

**E-mail:** rob.birchmeier@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:**

The National Aeronautics and Space Administration (NASA) Integrated Information Infrastructure Program (IIIP), under the management of the NASA Chief Information Officer (CIO), will provide the NASA workforce with the information infrastructure and tools that adapt and evolve to support management, science, research, and technology programs and eliminate the barriers caused by single solution systems.

Identity, Credential and Access Management (ICAM) manages identities, credentials, physical access, and logical access in an integrated, enterprise environment; thus, enabling NASA to ensure that individuals have the access they need to further the mission of NASA without putting Agency assets at risk.

The ICAM architecture is separated into: a) Identity Management; b) Credential Management and c) Access Management. Access Management has been split into Physical and Logical access. Identity Management deals with three major facets of an individual: basic details about the individual's identity (such as name and date of birth), the individual's affiliation with NASA (such as civil servant or contractor), and the knowledge NASA has about the individual based on investigations and record checks.

The National Aeronautics and Space Administration Identity Management and Account Exchange (IdMAX) system provides capabilities for NASA to manage identities for NASA Civil Servants and supporting individuals for accounts to access NASA logical and physical resources. IdMAX applications include NASA Access Management System (NAMS), Personal Identification and Verification (PIV), User Self-Service, and Remote Identity/users.

| 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. | U.S.C. Section 552a(b) Privacy Act of 1974, “Government Organization and Employees: Records maintained on individuals.”<br>NIST Digital Identity Guidelines (Special Publication 800-63 Suite)<br>M-05-24 "Implementation of Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors"<br>M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 Policy for a Common Identification Standard for Federal Employees and Contractors<br>M-16-04 "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government"<br>M-04-04 E-Authentication Guidance for Federal Agencies |

| | |
|---|---|
| | 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/privacy/nasa_sorn_10SECR.html |

| 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. | 2700-0158 |

| Privacy / Characterization of the Information | |
|---|---|
| Information is collected on the following: | NASA Contractors<br>Government Employees<br>Business Partners/Contracts, Grantees (including, but not limited to federal, state, local agencies) |
| Collection contains the following: | Name<br>Date of birth<br>SSN<br>Biometric identifier (fingerprint or voiceprint)<br>Other PII not listed above<br>Passport number<br>Driver's license number<br>Work phone number<br>Work cell phone number<br>UUPIC |

| | |
|---|---|
| | Work e-mail address<br>Home mailing address<br>Birth certificate<br>Legal documents (divorce decree, criminal records, etc.)<br>Photograph<br>Work Mailing Address<br>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. | Emergency Notification System (ENS) is a system used to notify NASA personnel of emergencies in their immediate area.<br>The Office of the Chief Health and Medical Officer (OCHMO) is implementing an electronic health record system (EHRS) for all the occupational health clinics in NASA.<br>OCHMO will use limited information to support the records of health of NASA users.<br>Human Capital Systems are the authoritative sources for civil servants identity data. |

| Privacy / Uses of the Information | |
|---|---|
| NASA will use the information in the following ways: | IdMAX uses identity information in order to create an identity record. Although the identity record is used primarily to gain access into NASA systems, these records may be disclosed to:<br>1. To the Department of Justice when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.<br>2. To a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an |

| | |
|---|---|
| | interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.<br>3. To an Agency in order to provide a basis for determining preliminary visa eligibility.<br>4. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.<br>5. To a staff member of the Executive Office of the President in response to an inquiry from the White House.<br>6. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. §§ 2904 and 2906.<br>7. To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.<br>8. To other Federal agencies and relevant contractor facilities to determine eligibility of individuals to access classified National Security information.<br>9. To any official investigative or judicial source from which information is requested in the course of an investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.<br>10. To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not |

| | |
|---|---|
| | constitute an unwarranted invasion of personal privacy, consistent with Freedom of Information Act standards.<br>11. To a Federal State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.<br>12. In order to notify an employee's next-of-kin or contractor in the event of a mishap involving that employee or contractor.<br>13. To notify another Federal agency when, or verify whether, a PIV card is no longer valid.<br>14. To provide relevant information to an internal or external organization or element thereof conducting audit activities of a NASA contractor or subcontractor.<br>15. Disclosure to a NASA contractor, subcontractor, grantee, or other Government organization information developed in an investigation or administrative inquiry concerning a violation of a Federal or state statute or regulation on the part of an officer or employee of the contractor, subcontractor, grantee, or other Government organization.<br>16. NASA standard routine uses as set forth in Appendix B. |
| 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. | All users must read and acknowledge the NASA Terms of Service and Paperwork Reduction Act. Additionally, individuals must read and acknowledge the Privacy Notice on guest.nasa.gov prior to entering in any identity information.<br>***"In order to submit your information for verification, please read and accept the following Privacy Statement:***<br>*Personally identifiable information, such as your name, social security nuber, date of birth and demographic information, such as your address and zip code, that you voluntarily provide to us (when you register with the Site) will only be utilized by NASA as a means of identity verification. Personal information is collected by NASA and provided to a contracted service provider strictly to assure identity verification/proofing and to ensure that increased access is not a threat to NASA applications. You are under no obligation to provide us with personal information of any kind, however, your refusal to do so may prevent you from using certain features within the approved applications."* |
| 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. | Federal employees and contractors who access NASA network and systems are required to have user identity in IdMAX. If an individual refuses to provide the appropriate information, they refuse access to NASA networks, systems and data.<br>The IdMAX system provides authoritative data and business process workflows to manage identities, credentials and access. Process details can be found in the IT-HBK-2841-03A, Identity, Credential, and Access Management Services (ICAM) Handbook in accordance with NPR 2841.1. |
| 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 | Creating a NASA Identity means generating a record in the Identity Workflow that establishes a relationship between the applicant and NASA. Individuals are responsible for completing all required fields, which is used to establish a Level of Confidence for an identity. The IdMAX User Handbook and ICAM Handbook IT-HBK 2841-003 provide further insight into the described process. |
| The IIF is collected | Mandatory |
| **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. | Federal employees and contractors who access NASA network and systems are required to have NASA user identity in IdMAX. If an individual refuses to provide the appropriate information, they refuse access to NASA networks, systems and data. Prior to providing identity information all users must read and acknowledge the NASA Terms of Service and the Paperwork Reduction Act in accordance with the ITS-HBK 2841-03A ICAM Handbook and NPR 2841.1 |
| Are individuals notified of the consequences of providing information? | Yes |
| If yes, describe the process. If no, explain why not. | Yes, the Privacy Policy states "<br>AUTHORITY: 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended<br>PURPOSE: To collect information from persons requesting access to NASA assets and/or resources in order to establish an identity and determine eligibility for access.<br>ROUTINE USES: Use and disclosure of your records within and outside of NASA may occur in accordance with the NASA Security Records System Privacy Act System of Record Notices published at https://www.nasa.gov/content/nasa-privacy-act-system-of-records-notices-sorns and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)).<br>DISCLOSURE: Providing this information is voluntary; however, failure to provide the requested information may result in the denial of access." |

| **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. | 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.<br>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.<br>The Emergency Data Records are maintained in Agency files and destroyed when superseded or obsolete in accordance with NRRS 1, Item 100B. Emergency Data 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.<br>The Criminal Matter Records are maintained in Agency files and destroyed in accordance with Items A and B of National Archives and Records Administration Disposition Authorization N1-255-07-2 after its approval by the Archivist of the United States. Criminal Matter 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.<br>The Traffic Management Records are maintained in Agency files and destroyed in accordance with Item C of National Archives and Records Administration Disposition Authorization N1-255-07-2 after its approval by the Archivist of the United States. Traffic Management Records may be obtained from the cognizant system or subsystem manager listed above. Requests must contain the following identifying data concerning the requestor: First, middle, and last name; date of birth; Social Security Number; period and place of employment with NASA, if applicable. |

| | |
|---|---|
| | |

| 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. | Trulioo uses real-time validation of identity information.  That information is accessed through a direct integration.  And the information is used temporarily while the validation is processing.<br>Background investigation information is provided to Office of Personnel Management (OPM) through a direct integration.  This process follows Federal ICAM (FICAM) best practices.<br>Finger print information is provided to Federal Bureau of Investigations (FBI)<br>Clearance Continuous Evaluation information is provided to the Office of the Director of National Intelligence (ODNI) through a direct integration. |
| 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."<br>**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. |
| What procedures are in place to allow the subject individual to correct inaccurate or erroneous information? | Users have access to the identity viewer in IdMAX and personnel information can be updated via id.nasa.gov.  For Personal Identity Records, Emergency Data Records, and Traffic Management Records, the NASA rules for access to records and for contesting contents and |

| | |
|---|---|
| | appealing initial determinations by the individual concerned appear at 14 CFR part 1212 - Privacy Act-NASA Regulations. |
| How does the project notify individuals about the procedures for correcting their information? | User procedures are provided to the applicable role holder or user. Online help is also available through id.nasa.gov. Per 10SECR (Notification Procedure), Information may be obtained from the cognizant system or subsystem manager. Requests must contain the following identifying data concerning the requestor: First, middle, and last name; date of birth; Social Security Number; period and place of employment with NASA, if applicable. |

## 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 IdMAX where all National Institute of Standards and Technology (NIST) 800-53 controls are investigated and validated. All audit logs from IdMAX systems are recorded and maintained for the length of time per NASA policy stated in ITS-HBK-2810.16-01. NASA Access Management System (NAMS) tracks all user access requests and are validated annually. |
| Describe what privacy training is provided to users either generally or specifically relevant to the project. | Role holders have specific training required by NASA.<br>New employees must take Introduction to Information Technology Security and Privacy Awareness for New Employees.<br>All NASA users are required to take an annual Cyber security and Sensitive Unclassified Information Awareness Training and acknowledge the Rules of Behavior. |
| What procedures are in place to determine which users may access the information and how does the project determine who has access? | The NASA Access Management System, controls the workflow approval and provisioning of user access. |
| 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? | Memorandum of Understanding (MOU) and Interconnection Service Agreements (ISA) are notated within the System Security Plan. These are reviewed and approved per the maintenance lifecycle. |

## 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). | Yes |

**Agency Privacy Manager (APM):**

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

**APM Review Decision**: Concur

**APM Review Date:** 10/01/2020

**Chief Privacy Officer (CPO):**

HARRIS HOULT, STAYCE D

**CPO Review Decision**: Concur

**CPO Review Date:** 05/05/2021

STAYCE HARRIS HOULT Digitally signed by STAYCE HARRIS HOULT
Date: 2025.03.24 15:50:10 -05'00'

CPO Digital Signature

**NASA Senior Agency Information Security Officer (SAISO):**

Witt, Michael

**SAISO Review Decision**: Concur

**SAISO Review Date:** 02/16/2022

**NASA Senior Agency Official for Privacy (SAOP):**

SEATON, JEFFREY M

**SAOP Review Decision**: Approve

**SAOP Review Date:** 02/16/2023